MiVoice MX-ONE

Optional Installations

Release 7.2

November 8, 2019

Notice

Trademarks

Contents

MiCollab Integration

This topic discusses the MiCollab integration with MX-ONE. For information on the MiCollab integration with MX-ONE see MiCollab Platform Integration Guide.

MiCollab Example Introduction

This document contains an example of basic installation and configuration of the MiCollab application server for integration with MiVoice MX-ONE.

Prerequisites

- Configure MX-ONE for MiCollab integration (see MX-ONE integration chapter in MiCollab Customer Documentation).
  - Configure PBX group and members in MX-ONE to be used for AWV.
  - Configure SIP trunk in MX-ONE using profile NuPoint (remember to use remote port=5058).
  - Configure csta link in MX-ONE.
- Used numbers and IP address in the examples:
  - Attendant number in MX-ONE: 09
  - MX-ONE IP address: 192.168.222.100
  - Internal number serie:4xxxx
  - Internal number length: 5 digits
  - NuPoint: Access number: 6001
  - Lines to NuPoint VoiceMail: 15
  - Lines for NuPoint MWI: 1
  - Lines for outgoing calls from NuPoint: 4
  - AWV Access number: 8003
  - Number of ports AWV: 3
  - SIP Port Extension numbers for AWV: 8004,8005,8006

OVA Deployment Installation

Do as follows:

Deploy the MiCollab .ova file:

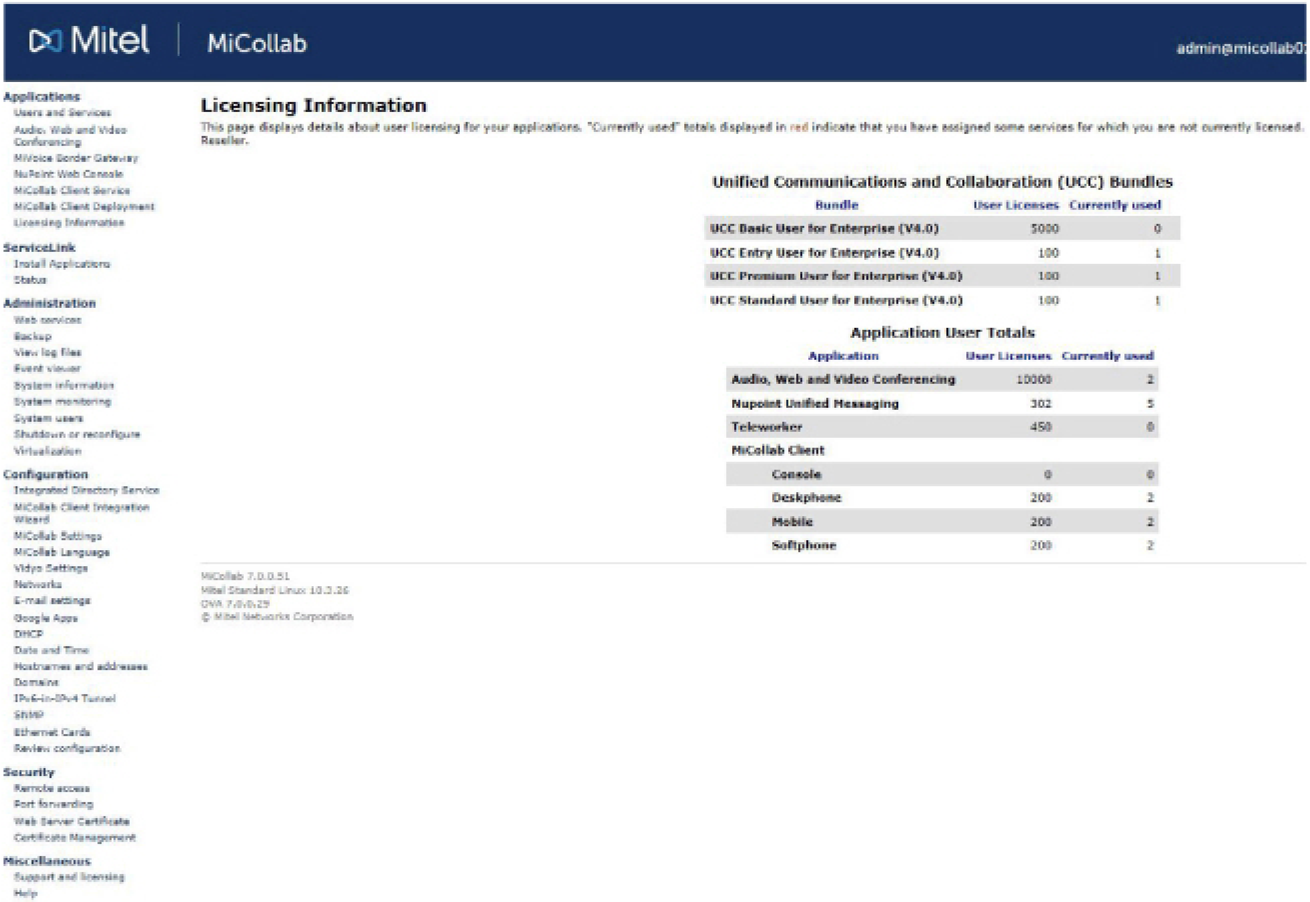
1. Start the virtual machine.
2. Open the console interface.
3. Choose keyboard.
4. Restore from backup - no.

5. Set Administrator's password (this is the same for both root and admin user).
6. Select Timezone - (e.g. CET).
7. Enter primary domain - (e.g. mydomian.com).
8. Enter system name - (e.g. micollab).
9. Select only eth0 - just now no WAN should be enabled.
10. Type the IP address of the server.
11. Type the netmask.
12. Do not configure IPv6.
13. Do not configure eth1.
14. Do not configure another local network adapter.
15. Type the default gateway for the server.
16. Type the IP address of the corporate DNS .
17. Select the corporate DNS for DNS resolution.
18. Wait for the configuration to be activated.
19. Enter ARID and IP address (Important use correct address) of the FMC and then select PBX type.
20. Login through the console interface as admin.
21. Select 9. Manage Trusted Networks.
22. Select 2. Add IPv4 trusted network.(e.g the internal corporate ip network segments).
23. Enter the subnetmask.
24. Enter the router to use for the trusted network - normally the same router as for the server.
25. Select Next, then Back to the menu.
26. Login to https://<fqdn>/server-manager with admin and password configured during installation.

Configuration of MiCollab

In the main window and from the left menu you administrate the configuration of the MiCollab, see below.Complete all configurations before start using PM to deploy users.

Figure 1.1: Main window



Menu: Service Link

- Select Service Link and then Status.
- If you have not entered your ARID (Service account id) during the initial installation then enter it now together with the ip.address of the FMC.

NOTE: If you have not selected the PBX during the initial installation, go to ServiceLink/Install Applications/Install Applications - select the PBX type and Next.

Menu: Configuration

- Select and start the MiCollab Client Integration Wizard.
- Select MiCollab Language Settings and set the System Language and Other NuPoint UM Prompt.
- Select E-mail settings. If required, configure settings for outbound SMTP server and userid.

Menu: Security

- Select Remote Access. If required, change Secure Shell Settings to allow SSH access for later diagnostics.

Menu: Administration

- Select System Users. For the account micollab api. select Reset password and enter a new password. You will require this user account and password when configuring the MiCollab subsystem in PM.

Menu Application

Menu application options are discussed in this section.

Option: Users and Service

Select User and Services and then configure following options:

- Option: Network Element
  a. Select Add.
  b. Type =MiVoice MX-ONE
  c. System Name= <my Mxone>
  d. IP Address = 192.168.222.100
  e. Call Forward Destination Number = 6001
- Option: User templates
  – Select Add.

    Create customer roles templates from available default templates. It’s done by selecting wanted default template, creating a copy of it and save with a new name. Edit the created customer templates for Entry, Premium, Standard and Standard - Mobile.
  – Entry
    - Select TUI Passcode. TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more). TUI Passcode = Use this value = 4-10 digits (if extension length is less than 4 digits).
    - Attendant Extension: 09
    - Message Waiting #1 = DTMF to PBX
- Premium
  – Password = Use this value = "Strong Password"
  – Select TUI Passcode
  – TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more)
  – TUI Passcode = Use this value = 4-10 digits (if extension is less than 4 digits)
  – Attendant Extension: 09
  – Message Waiting #1 = DTMF to PBX
- Standard

- Password = Use this value = Enter a strong Password
- Select TUI Passcode
- TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more)
- TUI Passcode = Use this value = 4-10 digits (if extension is less than 4 digits)
- Attendant Extension: 09
- Message Waiting #1 = DTMF to PBX

- Standard - Mobile
  - Password = Use this value = Enter a strong Password
  - Select TUI Passcode
  - TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more)
  - TUI Passcode = Use this value = 4-10 digits (if extension is less than 4 digits)
  - Attendant Extension: 09
  - Message Waiting #1 = DTMF to PBX

Option: MiCollab Client Service

Select MiCollab Client Services and then Configure MiCollab Client Services. Configure following options.

PBX Nodes.

- Select the PBX Node and configure.
- Set length: 5 (internal number length in the MiVoice MX-ONE).

Enterprise

- Select Enterprise and then Default Account Settings.
- Select appropriate Country from the drop-down list

Option: Audio, Web and Video Conferencing

Select Audi, WEB and VIDEO conferencing and configure following options.

Configure SIP Server

- Select Add and configure, MX-ONE SIP Server Configuration.
  Extension first: 8004
  Extension last: 8006
- SIP password: 8003 (if authorization code is set to 8003 in MX-ONE for the extensions 8004-8006)
- SIP Domain: mydomain.com (domain of MX-ONE)
- IP Address: 192.168.222.100
- SIP Port: 5060

Web Conferencing Settings

- Select and configure Web Conference Name.
- Web conferencing Name: micollab.mydomain.com

System Options

Select and configure System Options:

- Platform - MiVoice MX-ONE
- Dial -in phone number 1: 8003 (Internal number to AVW)
- Dial - in Phone Number 1 Label: internal
- Dial-in Phone number 2: 8468003 (corporate number to AWV)
- Dial- in Phone number 2 Label: corporate
- Dial -in number 3 +4684428003 (Public number to AWV)
- Dial- In Phone number 3 Label: Public
- Webserver admin E-mail system.admin@mydomain.com
- Generate Alert E-mail system admin@mydomain.com
- Prompt for Access Code first: Enable checkbox
- Allow HD Video Resolutions: Enable checkbox
- Prompt to extend conference 5 minutes prior to its end time: Enable checkbox

Option: NuPoint Web Console

Select and NuPoint Web Console and configure following options

Offline Configuration

Select Offline configuration/Edit Offline configuration and Duplicate Active Configuration - yes

Then select and configure following items:

1. Network Elements/Add
   a. Type = SIP GATEWAY
   b. Name = Mxone
   c. IP Address = 192.168.222.100
   d. Number of Ports = 20

2. Dialers (Pagers) (for Request playback call feature in UCA client) and select:

   a. Add a "dialer"
   b. Number: Select Next Available
   c. Enter a name - Dialer
   d. Acces code: T
   e. Hold Time : 20
   f. Add

3. Line Groups/Add

   a. Add a line group for Voicemail connection:
   - Line Group Number = 1
   - Name = VoiceMail
   - Application = NuPoint Voice
   - User Interface = NuPoint Voice
   - Lines/Add
   - Line Triplet - next Available

- Number of lines = 15
- PBX = MX-ONE
- Mapping = 1 (0 must not be used, see Online help - “add at Line Group)
- "Save"
- Pilot Number = 6001
- Dialling Plan
- Length of extensions starting with...
- 4 = 5 digits
- Voicemail
- System Attendent's extension = 09
- Save

b. Add a line group for Message Waiting indication:

- Line Group Number = 2
- Name = MWI
- Application = DTMF to PBX Dialler
- User Interface = NuPoint Voice
- Lines/Add
- Line Triplet - next Available
- Number of lines = 1
- PBX = MX-ONE
- Mapping = 16
- Add
- Pilot number = 6001
- DTMF to PBX Dialler/DTMF to PBX Dialer
- Pre-DN On Dial String = 1
- Pre-DN Off Dial String = 0
- Save

c. Add a line group for Outgoing calls from NuPoint:

- Line Group Number = 3
- Name = Outgoing Dialler
- Application = Outbound (Pager) Dialer
- User Interface = NuPoint Voice
- Lines/Add
- Line Triplet - next Available
- Number of lines = 4
- PBX = MX-ONE
- Mapping = 17
- Add
- Pilot number = 6001
- Save
- Dialling Plan
- Length of extensions starting with...

- 4 = 5 digits
- Select the Dialer(Pagers) created in step b) by selecting the checkbox
- Save

4. Select Commit Changes and Exit and then Activate.

Active Configuration/Line Groups

- Select Active Configuration/Line groups and then Edit line group for Voicemail (Linegroup 1)
- Check that Prompt Language 1 is set to default (Do not change this).

Class of service Feature COS/14. MAS

- Select Class of Service/Feature COS and then Edit FCOS number 14 (MAS)
- Enable checkbox for:
  - 051 Do not switch language for outside callers
  - 218 Passcode NOT needed on direct calls
  - 263 Store Caller Line Id as a phone or mailbox number
  - 264 Play outside caller user interface (with FCOS bit 280)
  - 280 Enable CLI Outside caller interface (with FCOS bit 264)

Test Access to AWV and NuPoint

- Call Voice Mail (access number 6001). Get Welcome message.
- Call to AWV (access number 8003). Get prompt to enter conference code.

MiCollab Advanced Messaging

Customer Product Information of MiCollab Advanced Messaging, see Product Documentation.

Mitel CMG

Customer Product Information of Mitel CMG, see Mitel InfoChannel

Mitel InAttend

Customer Product Information of Mitel InAttend, see Mitel InfoChannel

MiContact Center Enterprise

Customer Product Information of MiContact Center Enterprise, see Product Documentation.

Mitel MC Controller

Customer Product Information of Mitel MC Controller, see Product Documentation.

Mitel Performance Analytics

Customer Product Information of Mitel Performance Analytics, see Product Documentation.

Introduction

Brief description of mitel Performance Analytics

The Mitel Performance Analytics (MPA 2.1, former MarWatch) monitoring system provides fault and performance management for multiple enterprise VoIP systems and associated network infrastructure, both LAN and WAN. MPA supports monitoring and remote access, both for private networks, such as enterprise LANs and MPLS VPNs, and for public network or Internet-reachable devices, such as access routers.

MPA can monitor any SNMP device regarding alarms and general status.

MPA is a product from Martello Technologies.

Supported Scenarios

For an MX-ONE system with a single Service Node, the MPA shall of course be connected to that Service Node.

The MPA can be connected in a couple of different ways to a multi-server MX-ONE system.

The primary multi-server scenario is that each Service Node server is connected to a MPA probe.

Figure 1: Primary scenario, direct connection to all MX-ONE servers in a 4-server MiVoice MX-ONE system

Another possibility is that one Service Node can act as a proxy for several other Service Nodes (and other entities), in which case only the proxy Service Node will be connected to the MPA probe.

The second scenario is not recommended, since it has certain resiliency problems, due to the fact that the monitoring function will be fully dependent on the proxy, so if the proxy goes down, the status of the other nodes will not be reported.

You can also have a mix of the primary and secondary scenarios.

Figure 2: Secondary scenario, connection by proxy, connection only to one MX-ONE Service Node.

Prerequisites

MPA consists of a number of web services running on either a cloud-hosted computing platform or on-premises computing platform. There are several components to MPA. The remote ‘Probe’ installed in non-Internet accessible networks maintains databases of status and events, and provides a web portal with access security. Additionally, MPA has a Remote Access Service that provides a secure “cross-connect” for remote access to the customer network.

MPA 2.1 or later version shall be used.

The MiVoice MX-ONE system(s) shall be up and running on Linux (SLES), either on a cloud-hosted computing platform or on-premises computing platform. Appropriate MIB shall be active.

Mitel Performance Analytics SNMP integration with MiVoice MX-ONE

How to integrate with MiVoice MX-ONE

Do as follows:

1. As root open the file /etc/snmp/snmpd.conf.

2. Set the correct syslocation and syscontact to reflect where the server is located and who manages it.

3. Update the rocommunity setting to allow the Martello Marprobe to perform snmp-queries towards the MX-ONE.

4. Update the trapsink setting to point towards the Martello Marprobe. This should be done in all MX-ONE servers that the Martello MPA system should monitor.

5. After saving the changes you need to restart the snmpd daemon for the changes to take effect.

Example:(The Martello MPA probe has been assigned IP-address 192.168.157.128. To limit the access the “rocommunity” setting can be set to only allow access from a certain subnet or even a single IP-address).

Useful information

- Please see /usr/share/doc/packages/net-snmp/EXAMPLE.conffor a more complete example and snmpd.conf(5).
- Writing is disabled by default for security reasons. If you would like to enable it, uncomment the rwcom-munity line and change the community name to some-thing nominally secure (keeping in mind that this is transmitted in clear text).

Note! do not use ' < > in strings for syslocation or syscontact.

Note! If you define the following here you will not be able to change them with:

snmpset syslocation (Optional) Server Room on Floor 7.

syscontact Sysadmin (mxone-adminstrator@example.com).

They include all MIBs and can use considerable resources. See snmpd.conf(5) for information on setting up groups and limiting MIBs.

rocommunity public 127.0.0.1

rocommunity public 192.168.157.0/24

rwcommunity mysecret 127.0.0.1

MX-ONE alarm traps use the agentx protocol:

master agentx

AgentXSocket tcp:localhost:705

MX-ONE alarm traps can trigger snmptrapd to sent mail and textmessages rapcommunity:

Default trap sink community to use trapcommunity private

trap2sink: A SNMPv2c trap receiver

trap2sink 192.168.157.128

Co-existence with similar tools

Co-existence with similar tools
There are other tools for fault and performance management, for example the Manager System Performance application, that can also be connected to the MiVoice MX-ONE system, as long as different IP addresses are used compared to MPA’s.

However, there should be no need to have several such tools, so that is not recom-mended.

References

For further reading regarding MPA and its features and configuration options, please see MPA System Guide, Release 2.1 or later.

MiVoice Call Recording

Customer Product Information of MiVoice Call Recording, see Product Documentation.

Microsoft Products

This topic discusses the integration of MX-ONE with the Microsoft products described in the following sections:

Introduction

The MiVoice MX-ONE communication system is based on an open software and hardware environment that uses standard servers with a Linux SUSE operating system. This open standards approach enables Mitel to offer our customers the choice of integrating MiVoice MX-ONE latest Microsoft UC products. We have worked with Microsoft to ensure that this possibility is workable.

MiVoice MX-ONE 5.0 is the first communications system (IP-PBX) to be fully Unified Communications Open Interoperability Program (UCOIP) qualified with Skype for Business Server 2019. The integration of MX-ONE with Microsoft products is a complete Direct SIP Integration, including security and media bypass, enabling customers to have both MX-ONE 5.0/6.x and Microsoft Lync 2019 co-exist in the same infrastructure and thereby derive the benefits from the best of both worlds. MX-ONE integrates with Microsoft UC solutions directly via a SIP connection to reduce the overall cost and complexity of the combined solution.

Refer to Microsoft's TechNet site for "Infrastructure Qualified for Microsoft Lync" for more information about the Microsoft Unified Communications Open Interoperability Program. **http://technet.microsoft.com/en-us/lync/gg131938**

General

Integration of MiVoice MX-ONE with Skype for Business Server 2019 is supported as a complementary solution providing end-user services, such as instant messaging and conferencing.

Microsoft Partner Program has certified the integration between MX-ONE communications system running the MX-ONE Service Node software 5.0 SP4 and Skype for Business Server 2019 through a Direct SIP connection. Also, later versions of MX-ONE can be integrated with Skype for Business Server 2019.

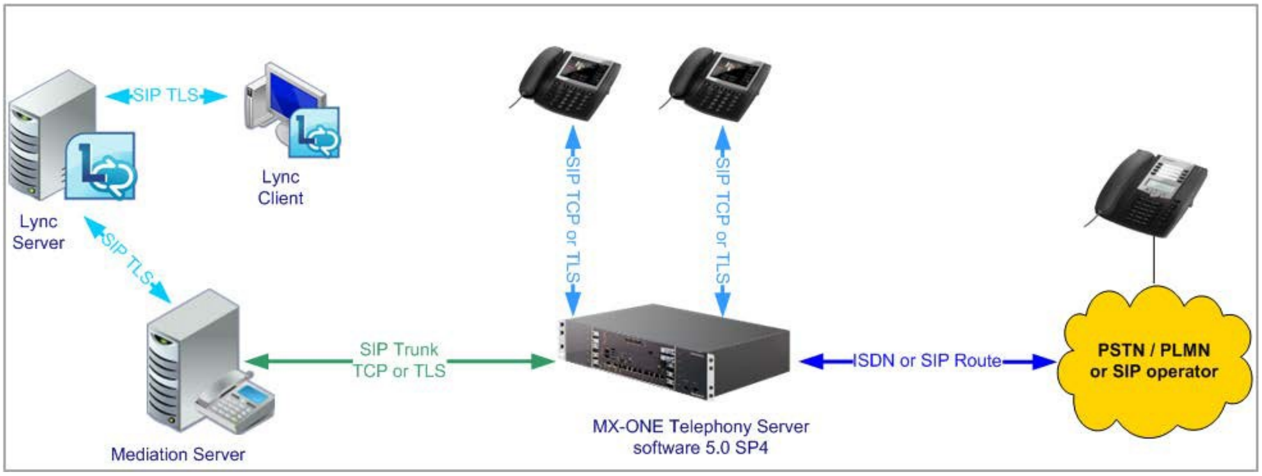
Scope

This guide describes the basic integration between MiVoice MX-ONE and Skype for Business Server 2019. The following sections describe the solution integration that has been certified through the Microsoft Partner Program and covers only the Direct SIP Integration. For more information about how this integration is set up and functions, refer to the relevant CPI documentation for MX-ONE, or go to the Microsoft UC product websites.

We recommend that you check the latest products documentation.

Integration Description

The integration of MiVoice MX-ONE and Skype for Business Server 2019 described in this guide is achieved via a Direct SIP that is specified by Microsoft. It means that a SIP trunk is used to connect MX-ONE and Skype for Business Server 2019 (Mediation Server). The SIP trunk connection between the systems can be deployed with or without encryption. MX-ONE supports TLS for signaling and SRTP for media encryption when connected with Mediation Server.



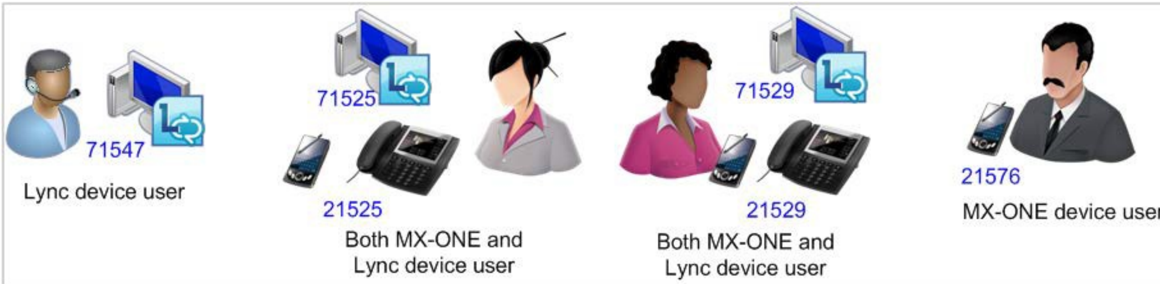
This guide covers only the components that are required in the integration between MX-ONE 5.0 SP4 or a later version, and Skype for Business Server 2019 via Direct SIP to offer the functionality required by the Microsoft UC Open Interoperability Program for enterprise telephony services and infrastructure.

At least the following Skype for Business Server 2019 components are required to support this integration:

- Server Infrastructure
  - Microsoft infrastructure (Domain Controller, Active Directory, DNS and so on)
  - Skype for Business Server 2019 Standard or Enterprise Edition
  - Microsoft Mediation Server
- Client
  - Microsoft Lync 2019

Direct SIP

In Direct SIP Integration, referred to as Enterprise Voice by Microsoft Lync 2019, users will have dedicated phone numbers that differ from those used in the MX-ONE.



This enables the Microsoft Lync 2019 client to make and receive external calls through a PC. The calls are routed from the Skype for Business Server 2019 by the SIP trunk to the MX-ONE and further to the PSTN and vice-versa. MX-ONE and Skype for Business Server 2019 will behave as networked PBXs, as typically is the case with all external trunks in the MX-ONE.

Direct SIP Signaling Overview

MiVoice MX-ONE supports SIP/TCP or SIP/TLS as the SIP transport mechanism when connected with Mediation Server.

The MX-ONE ports used for such connections are:

- SIP/TCP: 5060
- SIP/TLS: 5061

In addition to this, MX-ONE also supports media encryption (SRTP) when connected with Microsoft Lync 2019 Server when TLS is used. The media encryption is done between MX-ONE media gateway unit (MGU) and Microsoft Mediation Server or between MX-ONE media gateway unit (MGU) and Microsoft Lync client when Media Bypass is configured in Microsoft Lync 2019 Server.

Direct SIP Supported Features

During the certification process, the following Microsoft Lync features were validated with MX-ONE Service Node software 5.0 SP4.

- Basic Call services between MX-ONE and Lync end-points over SIP trunks:
  - Anonymous user calls
  - Caller ID on both ends
  - Decline call
  - Call forwarding and simultaneously ring feature
  - Inbound and outbound calls
- Media bypass (also known as direct media between MX-ONE and Microsoft Lync clients). Encryption (TLS and SRTP) is required for this functionality.
  - Inbound call from MX-ONE user device to Microsoft Lync client
  - Outbound call from Microsoft Lync client to MX-ONE user device
  - Outbound call: Call Forward All (CFA) to another Microsoft Lync client
  - Outbound call from Microsoft Lync to another Lync user; with bypass enabled and CFA enabled
- Outbound call: PBX CFB (Call Forward on Busy) to another Microsoft Lync user

  - Outbound call from Microsoft Lync to another Lync user; with bypass enabled and CFB enabled
- Conference
- Failover (to secondary Mediation Server - Lync gateway)
- Security (support for TLS/SRTP encryption)

Prerequisites

For proper integration between MiVoice MX-ONE and Skype for Business Server using Direct SIP, there are some prerequisites on both sides that must be fulfilled.

MiVOICE MX-ONE Requirements

On the MiVoice MX-ONE side, at least one MX-ONE Service Node and one Media Gateway are required to interwork with Skype for Business Server 2019.

Main Components

At least, the following MX-ONE components are required:

- MX-ONE communications system
  - MX-ONE Service Node
    - 5.0 SP4 or a later version
- Supported media gateways with the latest firmware compatible with 5.0 SP4, or a later version, which can be:
  - MX-ONE Classic - 7U 19-inch chassis, MGU board, or
  - MX-ONE Lite - 3U 19-inch chassis, using MGU board
  - MX-ONE Slim – 1U 19-inch chassis, using MGU board
- Terminals
  - All current MX-ONE terminal types are supported with this integration: SIP, H.323, analog, digital, DECT, and mobile extension

Licenses

The MX-ONE licenses needed for this integration are:

- SIP trunk licenses–note that the quantity of licenses depend on how the system is deployed).
- Encryption licenses are required if encryption (TLS/SRTP) is used.

Always check with your Mitel partner that your system has the required licenses, before beginning the integration deployment.

Skype for Business Server 2019

A Microsoft environment needs to be in place in the customer site. Note that Microsoft Lync is not part of the MX-ONE offering. It is important that expertise of Microsoft-competent engineers are available for installation and integration according to the MX-ONE configuration guidelines for the interface between the systems.

Main Components

The main Microsoft components that are required to interconnect with MiVoice MX-ONE are Skype for Business Server 2019, Mediation Server, and Lync clients. The Lync requirements are described in the Microsoft Lync Serve documentation. See the chapter References at the end of this guide.

NOTE: In Mitel´s lab validation, a single Skype for Business Server Standard Edition with a co-located Mediation Server was used. For testing load balancing and failover, two stand-alone Mediation

Servers were added to the topology.

Licenses

Microsoft licenses needed for this integration are described as they are beyond the scope of this guide.

Contact Microsoft or a qualified Microsoft partner to obtain the proper license requirements for each component of the Skype for Business Server solution.

Installation and Configuration

Installation

MiVoice MX-ONE Installation

Ensure that MX-ONE Service Node software 5.0 SP4 or a later version is installed in the customer environment. The system installation is not covered in this guide and must be performed by a qualified Mitel certified partner before the start of the integration work begins.

For Mitel MX-ONE installation, check the appropriate CPI documentation.

Microsoft Infrastructure

Ensure that Microsoft infrastructure and Skype for Business Server are installed in the customer environment by a qualified engineer.

For Microsoft infrastructure and Skype for Business Server requirements, check the appropriate Microsoft documentation.

Configuration

The following information was used in Mitel's laboratory setup during the validation of the solution. The setup may change depending of the customer specific needs.

NOTE: Fully Qualified Domain Name (FQDN) needs to be properly specified in the Domain Name System (DNS).

- MX-ONE 5.0 SP4 (or a later version)
  - Domain: lab.moon.galaxy Note that MX-ONE is part of a sub-domain
  - IP address: 192.168.222.10

    FQDN: mx-one-lync.lab.moon.galaxy
- Microsoft Domain Controller, Active Directory, Certification Authority, and DNS Server

  - Domain: moon.galaxy
  - IP address: 192.168.222.2

    FQDN: lync-infra.moon.galaxy

- Skype for Business Server Standard Edition and Mediation pool
  - Domain: moon.galaxy
  - IP address: 192.168.222.3

    FQDN: lync-2019-se.moon.galaxy

NOTE: Mitel recommends that complex scenarios be validated in the partner labs before customer deployment.

Direct SIP Setup

A SIP trunk must be configured in MX-ONE and the access code for this route (a trunk towards Skype for business).

MX-ONE uses ports TCP 5060 and TLS 5061 to be interconnected with Skype for Business Server 2019.

NOTE: MX-ONE 5.0 SP4 (or a later version) works with predefined SIP profiles for certain SIP service providers. if used, the profile file will help you in configuring the right data for the type selected. Each profile file may contain a number of profiles. The profile will preconfigure settings such as "-register", "-trusted", and so on according to the requirements of telephony provider.

MX-ONE 5.0 SP4 (or a later version) has predefined SIP trunk profiles to be used with Microsoft Lync 2019. One of the following trunk profiles needs to be selected during the MX-ONE SIP trunk configuration.

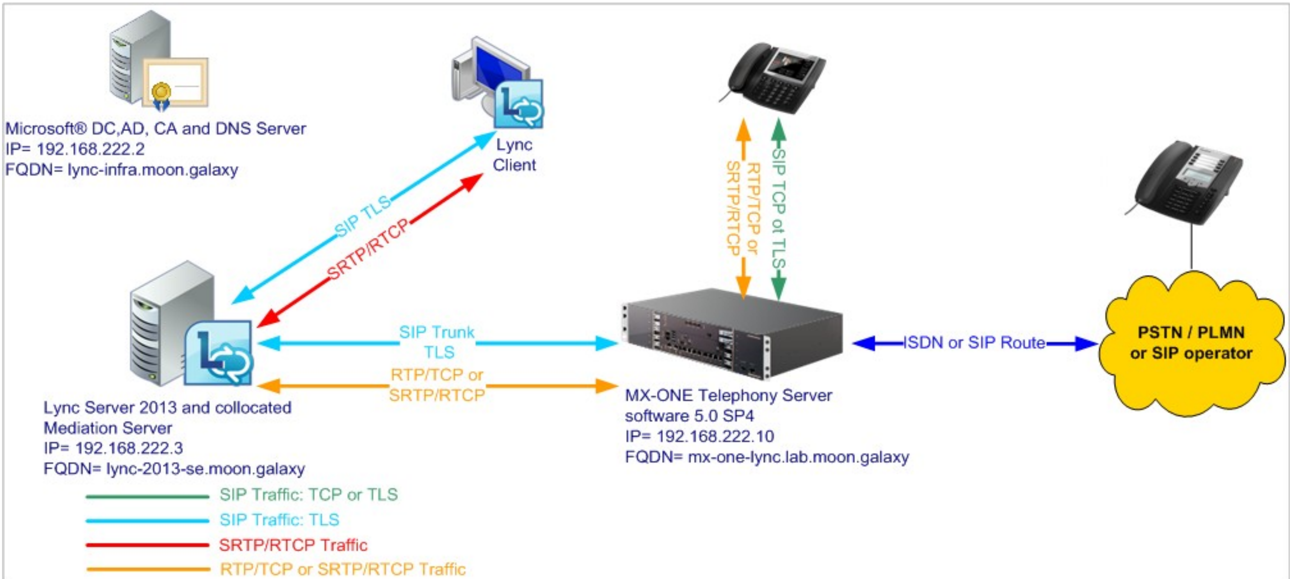
- Lync_TCP
  TCP is used as transport protocol; the listening port is 5068.
- Lync_TLS_SRTP. TCP is used as transport protocol; the listening port is 5067. SRTP is used to encrypt the media; it uses RTP/SAVP.

The following setup uses Lync_TCP where TCP is the transport protocol. In this case, the remote port is expected to be listening on port 5068.

To ensure a good interoperability between MiVoice MX-ONE and Skype for Business Server 2019, the SIP trunk profiles defined to Lync are “Forced Gateway”, at this guarantees the same behavior for all types of calls passing through MX-ONE and towards Skype for Business Server 2019.

MiVoice MX-ONE Direct SIP Setup - TCP

The following figure shows the Direct SIP Configuration used in this guide.



The following setup needs to be done in MX-ONE for configuring Direct SIP. Note that only SIP Route definitions are shown.

1. Use the following command to view more details regarding the SIP Profile Lync_TCP:
   `sip_route -print -profile Lync_TCP`
2. Define SIP Route category:

   ROCAI:ROU=99,SEL=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=001100;
3. Define SIP Route data:

   RODAI:ROU=99,TYPE=TL66,VARC=00000000,VARI=00000000,VARO=00000000;
4. Define SIP trunk data specific:

   sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;
5. Verify your configuration:

   sip_route -print –route 99 –short
6. Define the SIP Route equipment initiate; for example:

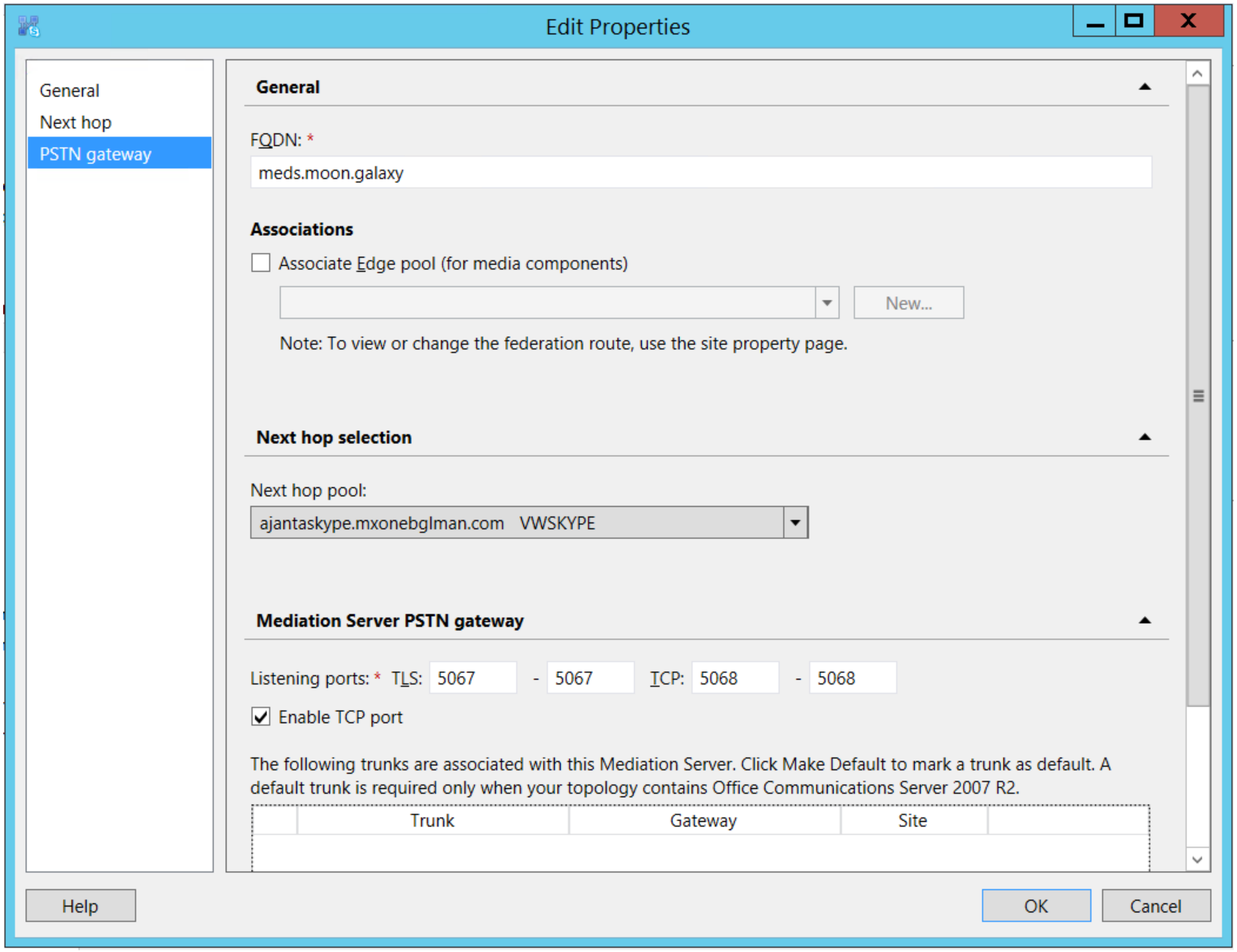
   ROEQI:ROU=99,TRU=1-1&&1-30;
7. Define external destination SIP Route data:

   RODDI:ROU=99,DEST=99,ADC=0005000000000250000001010000,SRT=3;

Skype for Business Server 2019 Configuration -- TCP

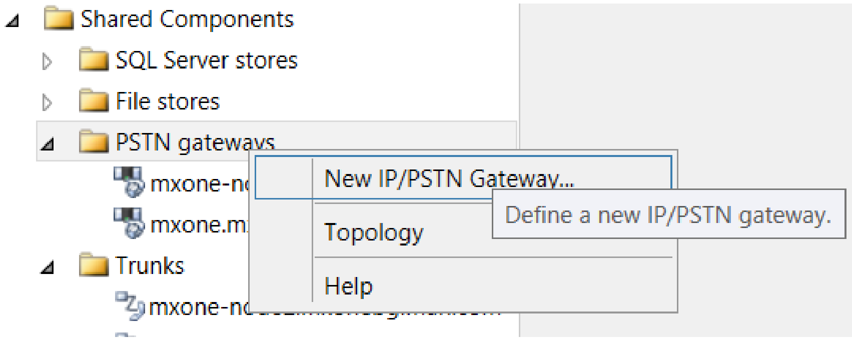
To finalize the configuration between MX-ONE and Skype for Business Server 2019, do the following:

1. Enable TCP port for the Mediation pool (disabled by default).

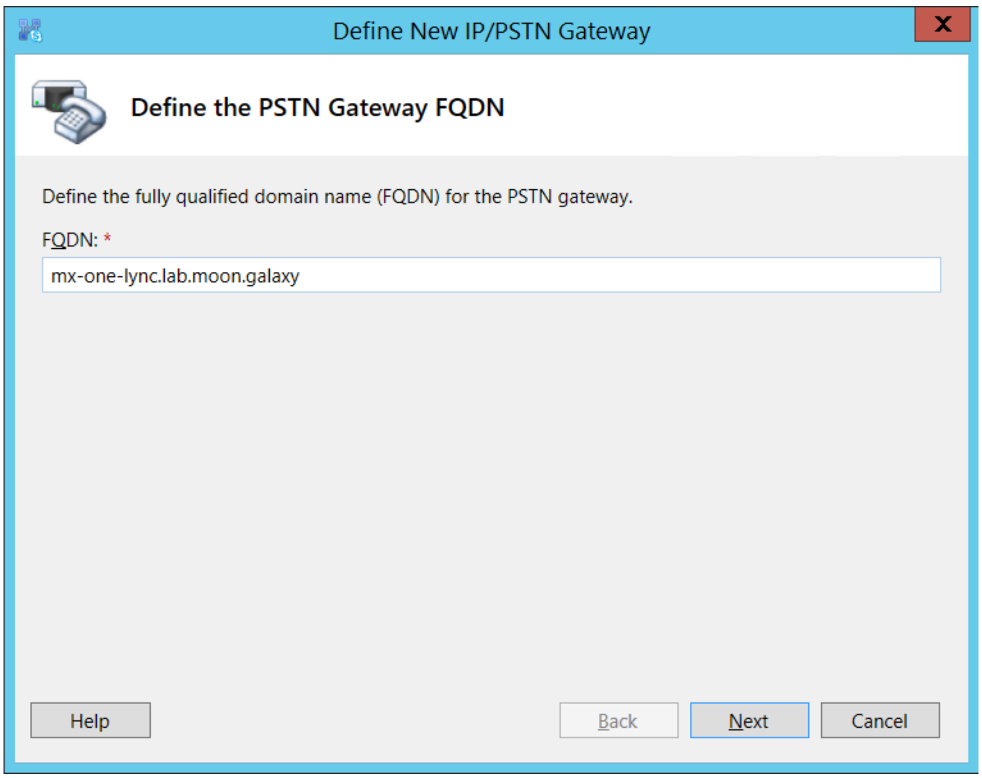


Define PSTN Gateway in the Skype for Business Server 2019 Topology Builder

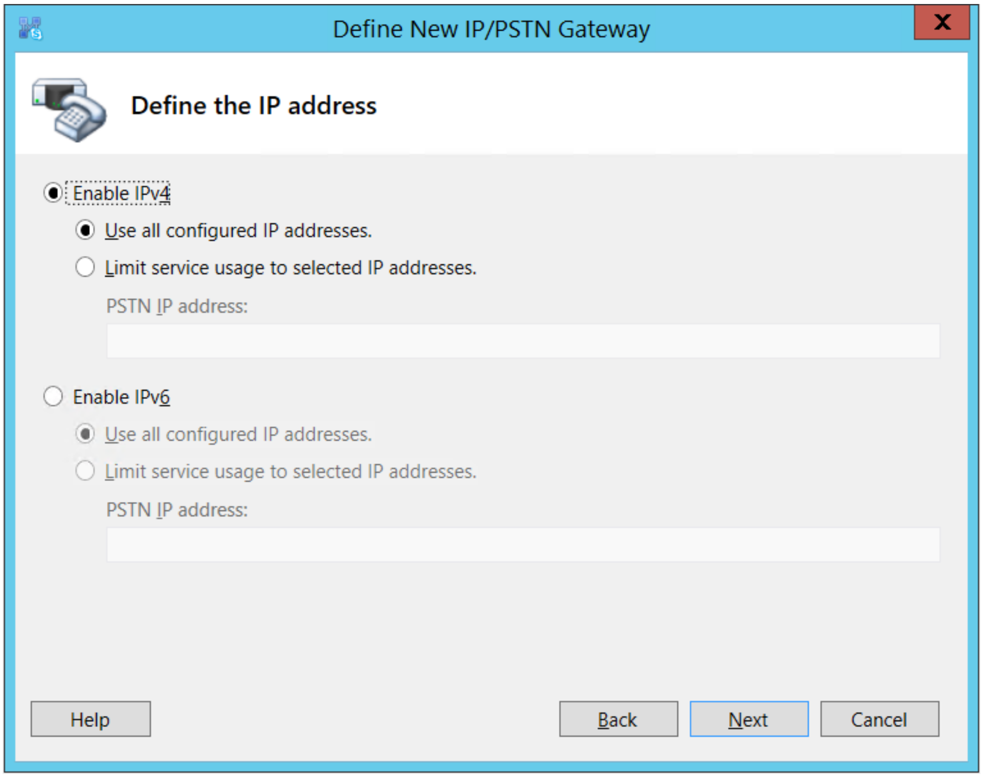
1. Open Skype for Business Server 2019, Topology Builder, and define a PSTN gateway to be used between Lync and MX-ONE.
2. To define the PSTN gateway, expand Shared Components, right-click **PSTN gateways**option.



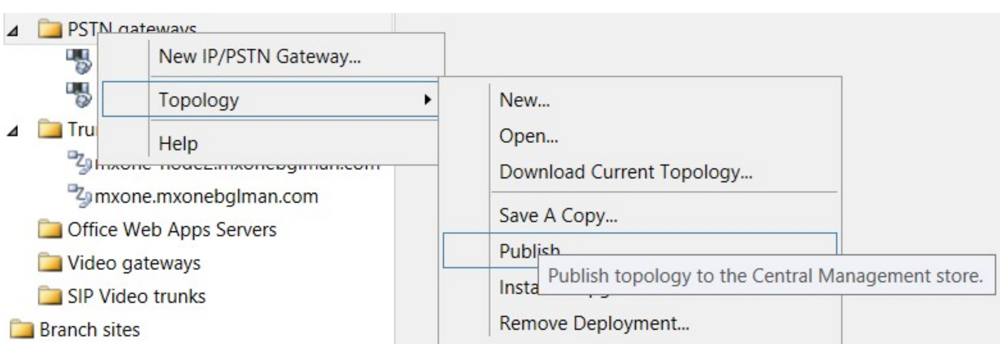
3. Click **New IP/PSTN Gateway**. The dialog box opens the Gateway FQDN or IP Address. Specify the MX-ONE IP Address or **FQDN** and click **Next**.



4. Define the IP address: in this example, the default is retained. Click **Next**.



5. **Define the root trunk**:
    - **Trunk name**: FQDN (MX-ONE FQDN)
    - **Listening port for IP/PSTN gateway**: 5060 (MX-ONE SIP TCP port)
    - **SIP Transport Protocol**: TCP
    - **Associated Mediation Server**: lync-2019-se.moon.galaxy
    - **Associated Mediation Server port**: 5068 (default)
6. Click **Next**.
7. Publish the **Topology**.



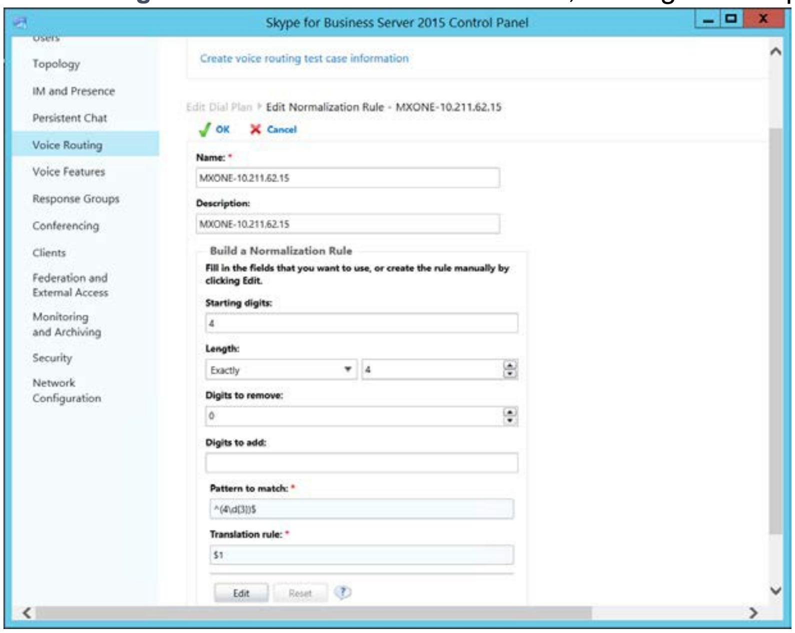
Define a Dial Plan

The **Dial Plan** configuration is required to allow Microsoft Lync users to dial to MX-ONE terminals and PSTN.

To define it, execute the following:

1. Open the Skype for Business Server Control Panel.
2. Click **Voice Routing** and choose **Dial Plan**.
3. Define Normalization rules that fits your organization needs. A rule for Lync users to dial to MX- ONE terminals and another to dial to PSTN (ensure that MX-ONE is connected to PSTN) are required. If needed, contact Microsoft for the appropriate setup for your requirement.

Figure 9.1: New Normalization Rule, five digits example



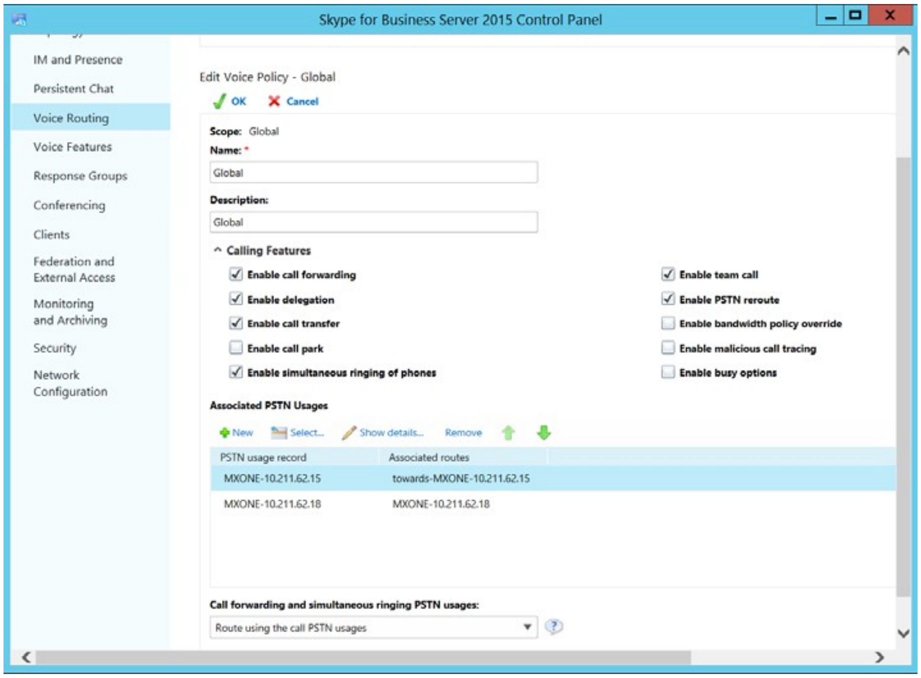
4. Commit the changes.

Define Voice Policy

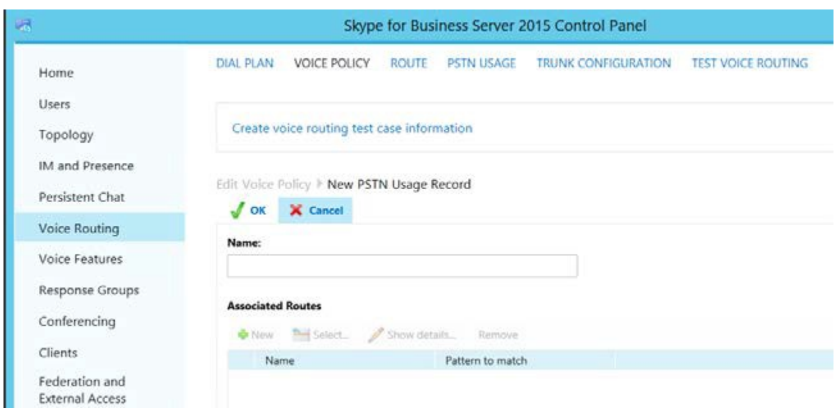
A voice policy is required to enable Microsoft Lync users to dial out via the Direct SIP connection using MX-ONE. Lync client users need to be assigned for this policy.

To Create the Voice Policy, do the following:

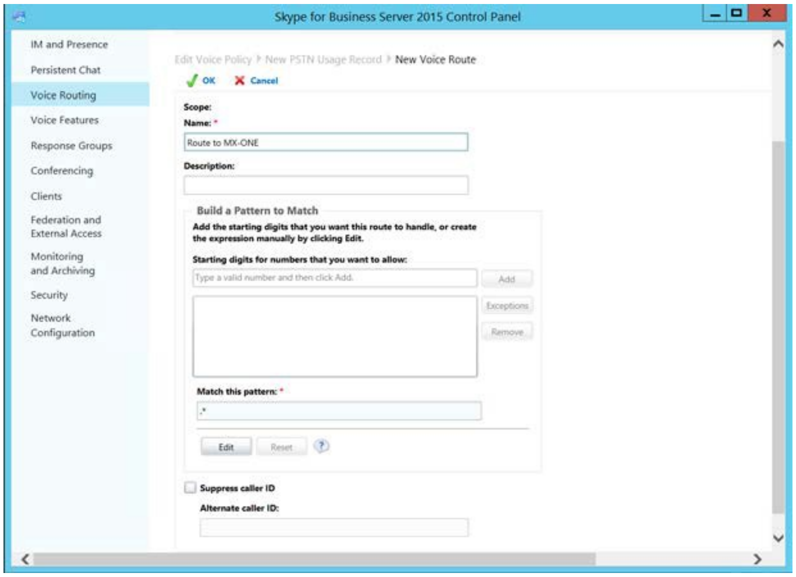
1. Click **Voice Routing** and choose **Voice Policy**.
2. Click **New** and choose the type of policy that is applicable for your company setup, site policy or user policy.
3. Enter a **Name** and a **Description** for the voice policy.



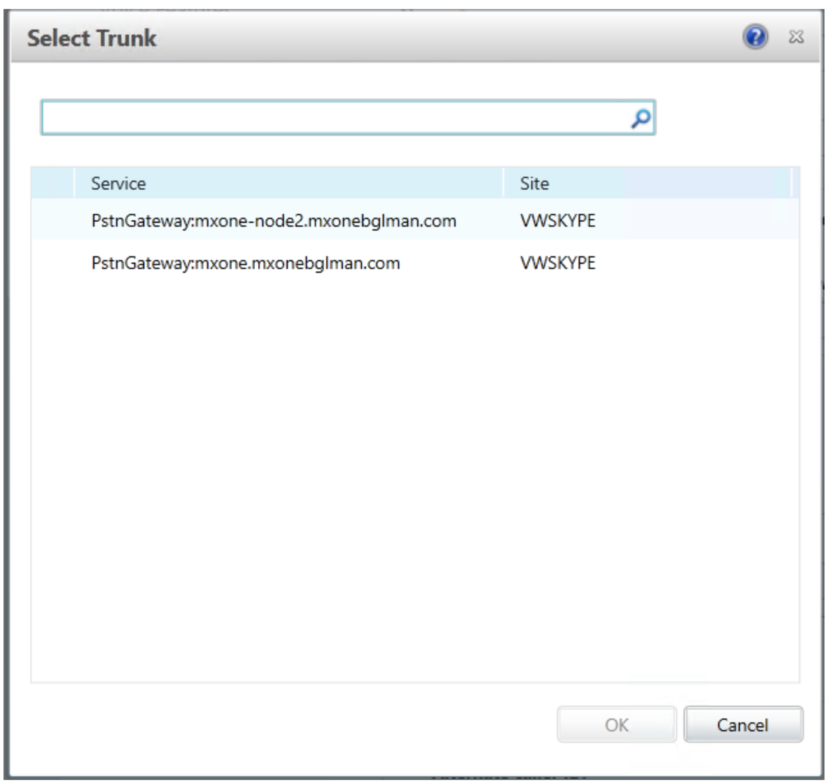
4. Associate a new PSTN for the policy and click **New**.
5. Enter a **Name** and a **Description** for the **New PSTN Usage Record**



6. Click **New** to associate a route with this PSTN usage record.
7. Enter a **Name** and a **Description** for the new Route.
8. Associate the MX-ONE gateway that you created earlier with the new **Route**. To do this, click **Add in Associated Gateways**.



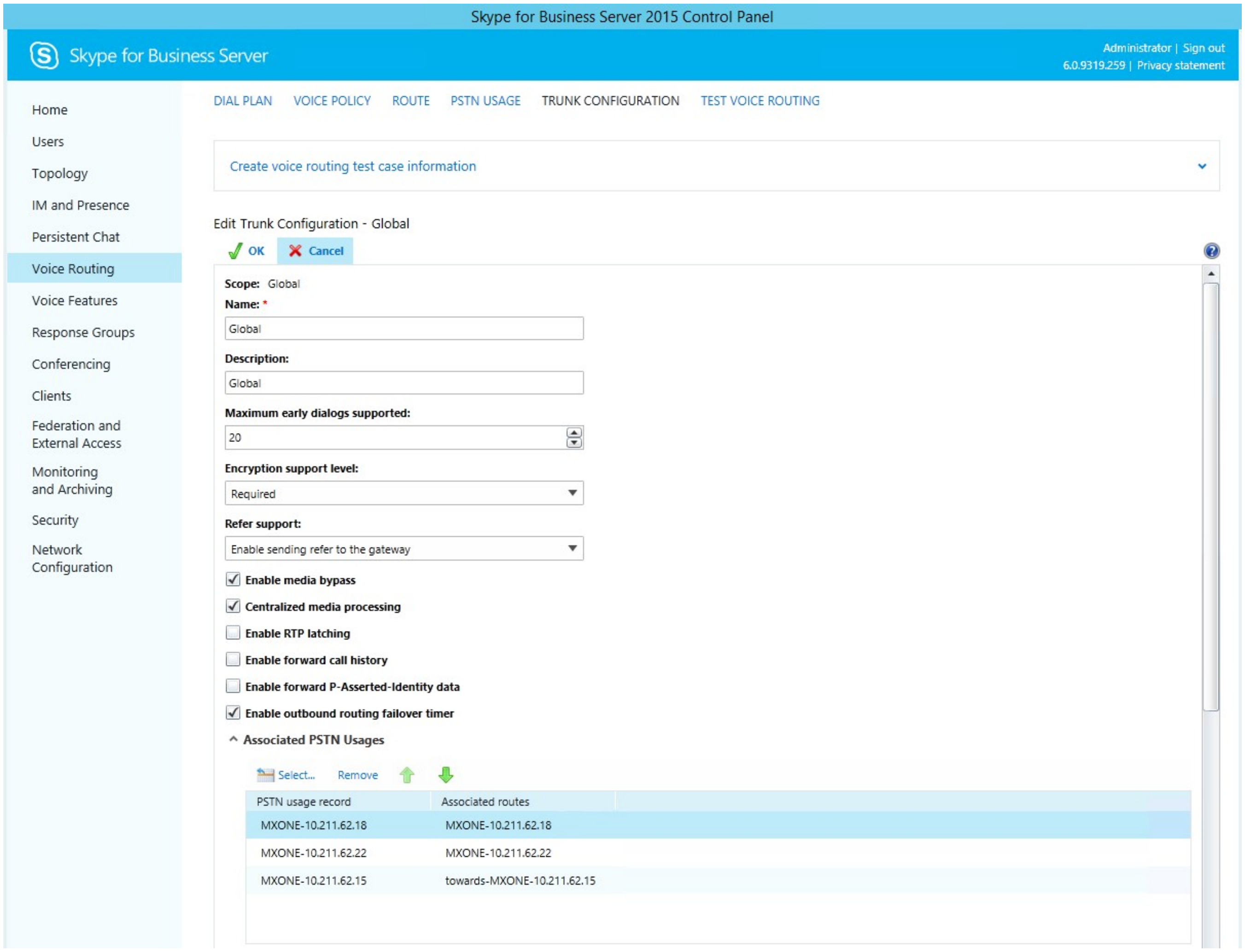
9. In **Select Gateway**, select the MX-ONE gateway created previously.
10. Click **OK** for all the queries to retain the configurations made.
11. Commit all changes.



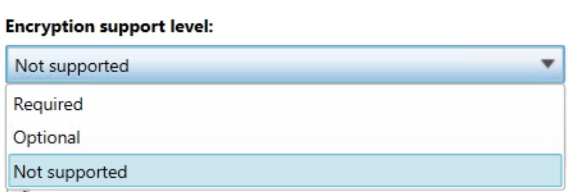
Define Trunk Configuration

To assign the MX-ONE gateway to a site or pool trunk, follow these steps:

1. Click **Voice Routing** and then click **Trunk Configuration**.
2. Click **New** and choose the type of trunk that is applicable for your company setup, site trunk, or pool trunk.



3. Select the **Encryption support level**. In this case, it is **Not supported**.



4. Commit all changes to complete the setup.

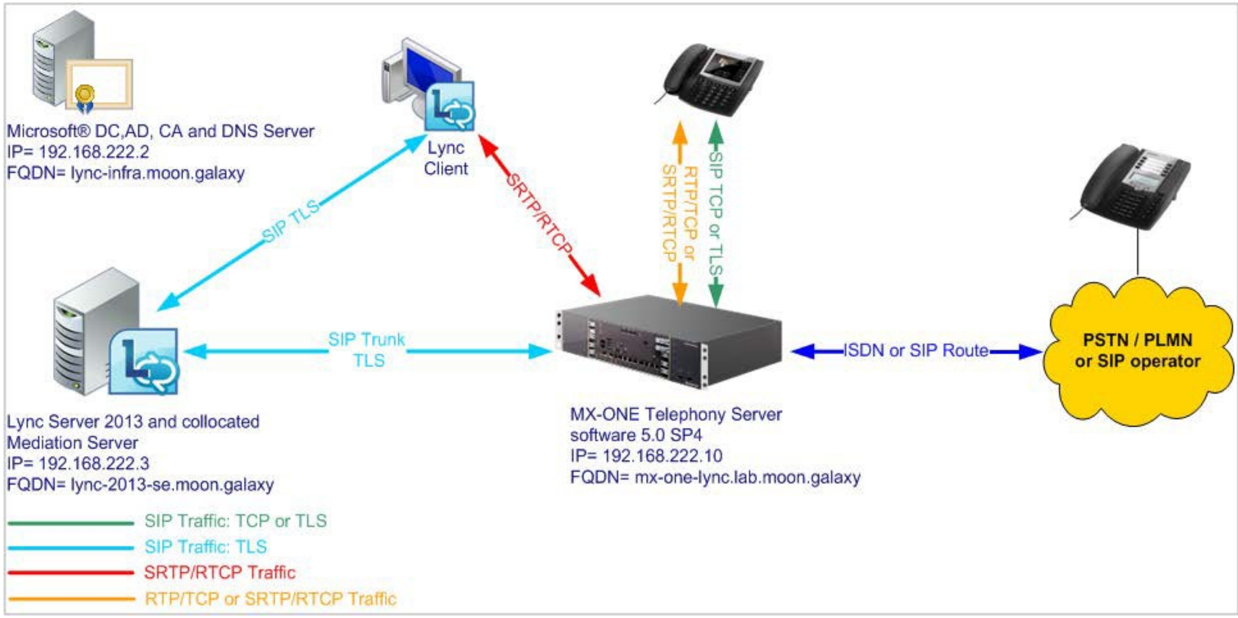
Conclusion

Now the setup is complete, assign users to the Policy created previously and test the integration by making calls between the systems.

See the topic Enable users for Enterprise Voice in Skype for business Server at the following link: **http://technet.microsoft.com/en-us/library/gg413011.aspx**

Direct SIP with Security and Media Bypass Setup

The following figure shows the Direct SIP with security and Media Bypass configuration used in this guide.



MiVoice MX-ONE Direct SIP with Security and Media Bypass Setup

The following setup needs to be done in MX-ONE in order to configure Direct SIP with security (encryption). Note that only Route definitions are shown.

NOTE: MX-ONE FQDN needs to be properly defined in the DNS Server.

When using security, the appropriate certificate must be installed in MX-ONE in addition to the encryption licenses. Check Certificate Management on MX-ONE CPI documentation for more details regarding certificates.

NOTE: TLS/SRTP security is required for Media bypass functionality. It means that the proper encryptions licenses must be loaded in the MX-ONE system.

1. Use the following command to view more details regarding the SIP Profile Lync_TLS_SRTP:
   `sip_route -print -profile Lync_TLS_SRTP`
2. Define SIP Route category:

   ROCAI:ROU=98,SEL=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=001100;
3. Define SIP Route data:

   RODA I:ROU=98,TYPE=TL66,VARC=00000000,VARI=00000000, VARO=00000000;
4. Define SIP trunk data specific:

sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;

5. Verify your configuration:

   sip_route -print –route 98 -short

6. Define the SIP Route equipment initiate: ROEQI:ROU=98,TRU=1-1;

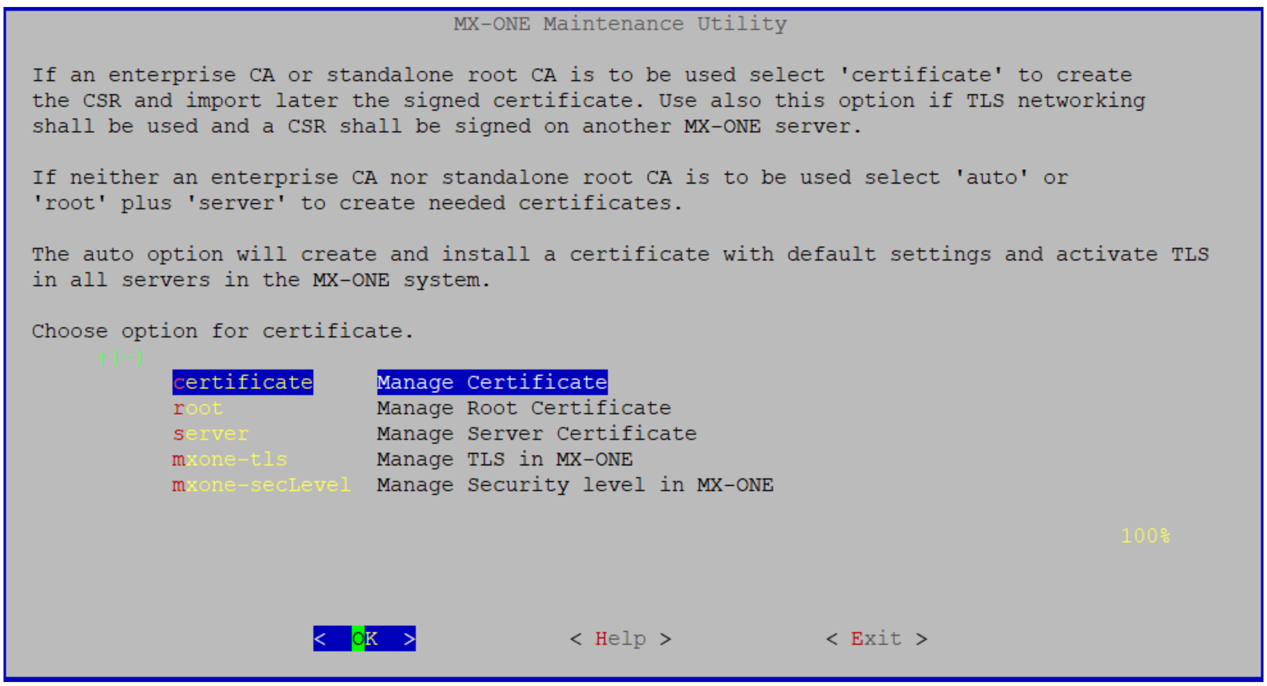
7. Define external destination SIP Route data:

   RODDI:ROU=98,DEST=98,ADC=0005000000000250000001010000,SRT=3;

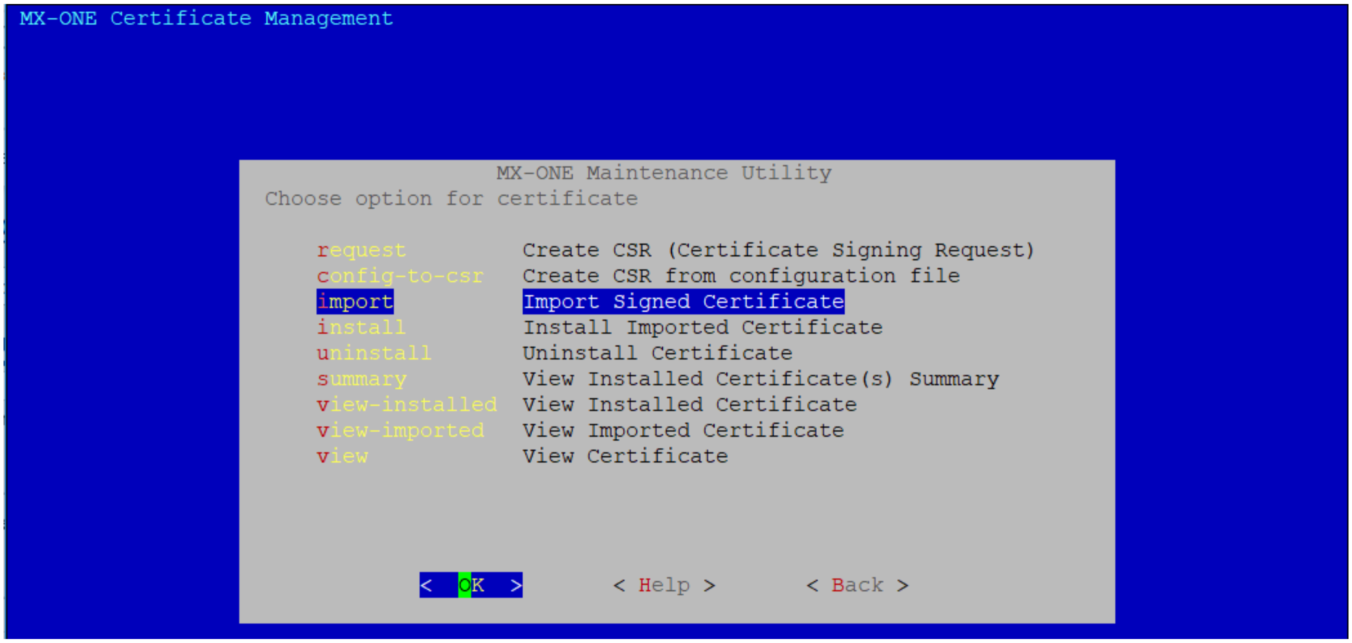
Import the Certificate to MX-ONE Service Node

Import the server certificate mx-one-certificate.pfx to MX-ONE Service Node.

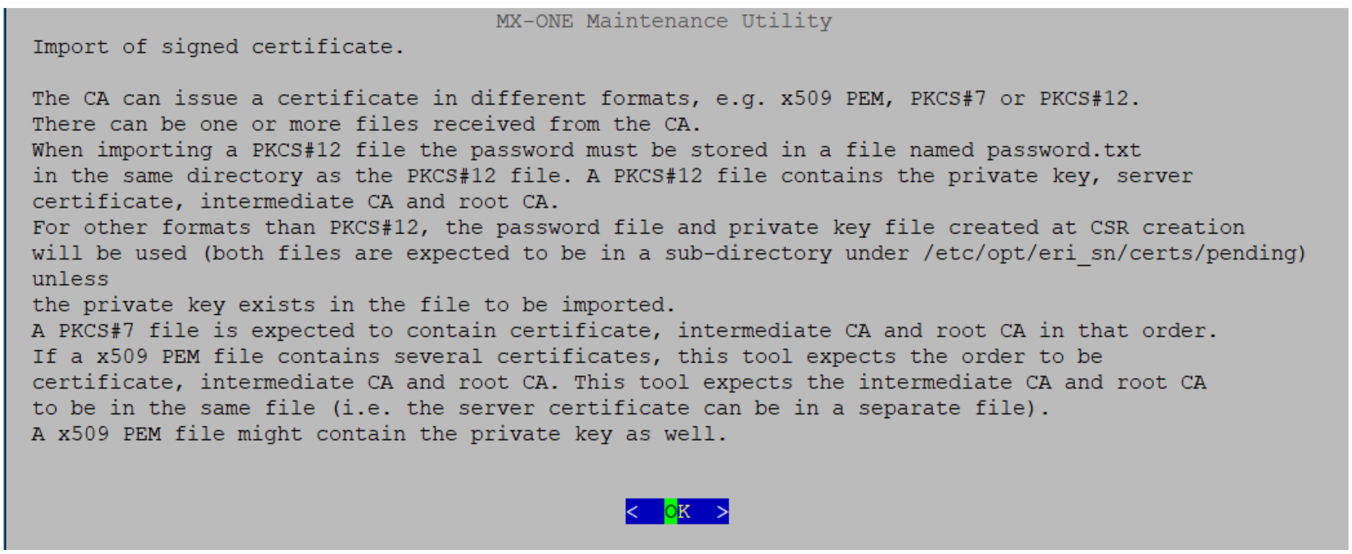
1. Install the certificate in the MX-ONE Service Node 1.
2. Run the mxone_certificate as root and press **Enter** button. The following screen appears.



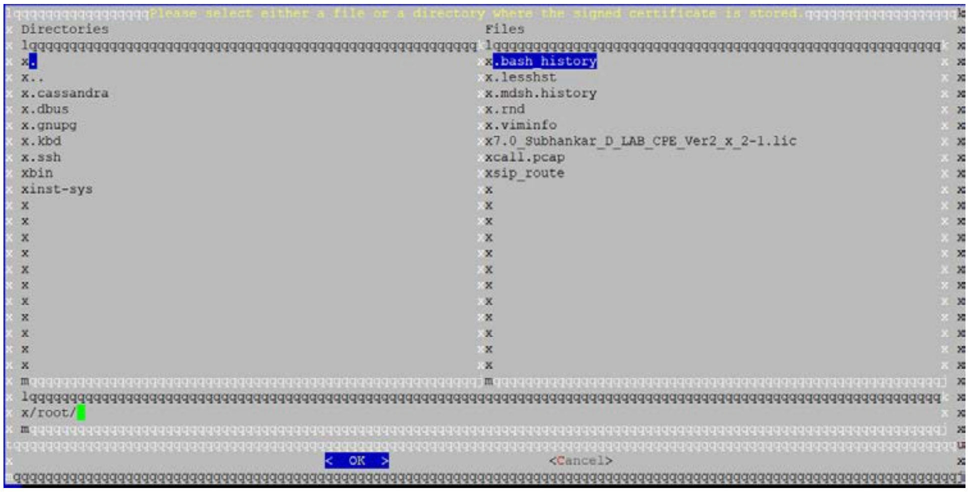
3. Select **certificate** and click **OK**. The following screen appears.



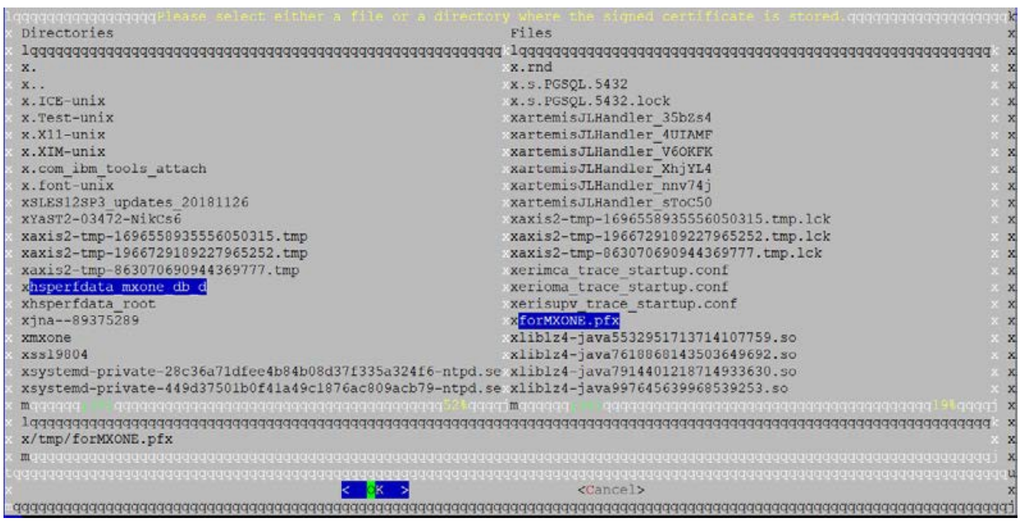
4. Select **import** and click **OK**. The following screen appears.



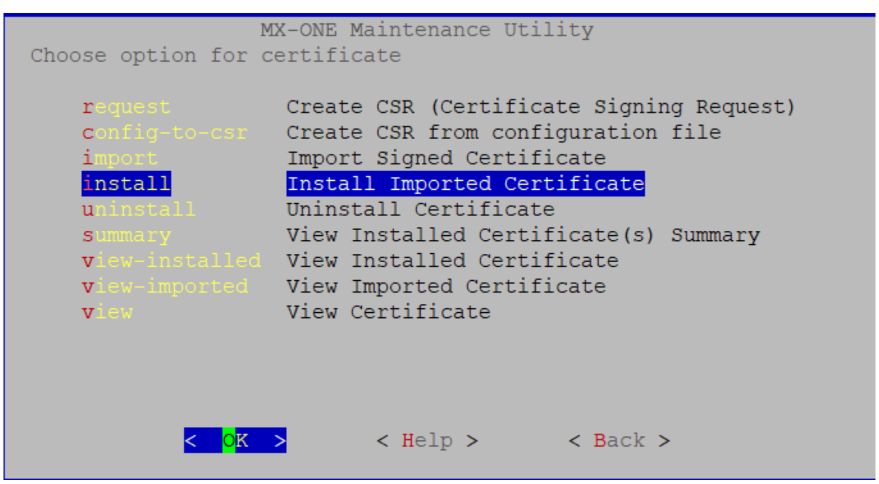
5. Click **OK**. The following screen appears to select a file or directory where the signed certificate is stored.



6. Specify the path where the **forMXONE.pfx** certificate is stored as shown in the following screen.



7. Click **OK** to store the imported certificate. Next, you install the certificate that you have imported and click **OK**.



```
                    MX-ONE Maintenance Utility
No imported certificate found.

To install root/server certificate (not the imported) do the following:

To install the root certificate, select root and then install and select not to
use imported root certificate.

To install the server certificate, select server and then install and select not
to use imported server certificate.

                         <  OK  >
```

8. Enable the TLS in MX-ONE > Manage TLS in MX-ONE -> Configure MX-ONE to use TLS. Refer to the 132/154 31-ANF 901 14 document for more detail.

9. Enable Media Encryption in the route:

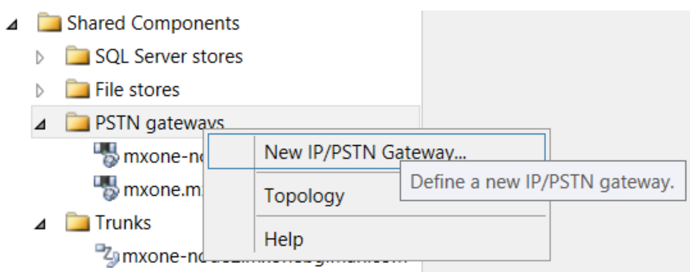
   media_encryption_enable -type route
   media_encryption_enable -type extension
   media_encryption_enable -type intermgw
   media_encryption_print

Lync Configuration with Security and Media Bypass Setup

You must do the following to finalize the configuration between Mitel MX-ONE and Skype for Business Server 2019 the following needs to be done:

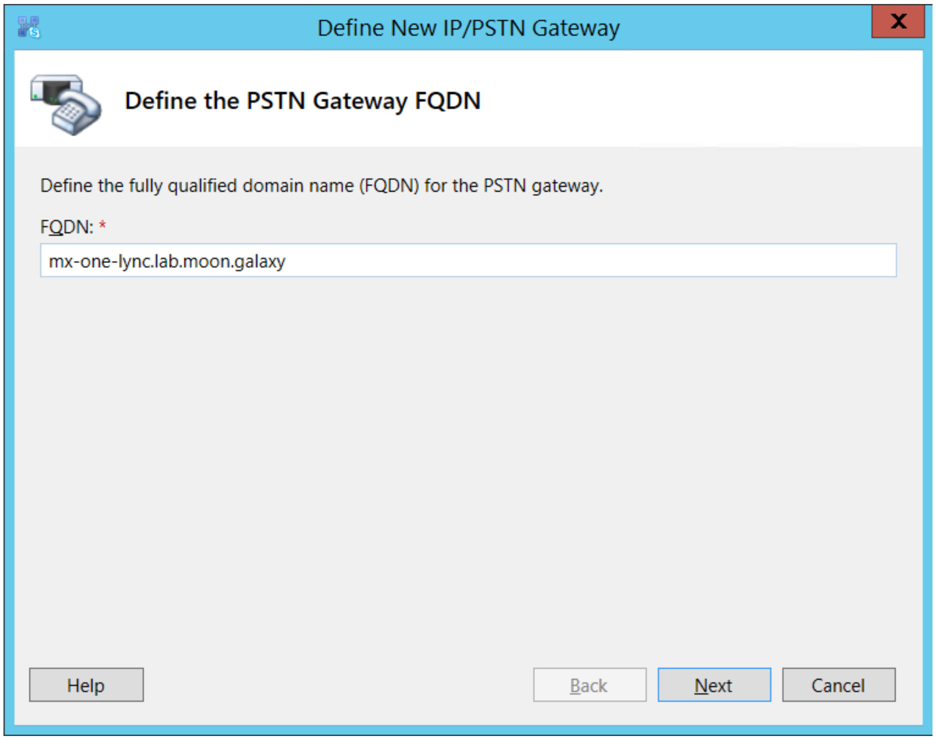
Define PSTN Gateway in the Skype for Business Server 2019 Topology Builder

1. Open the Skype for Business Server 2019, Topology Builder, and define a PSTN gateway be used between Lync and MX-ONE.

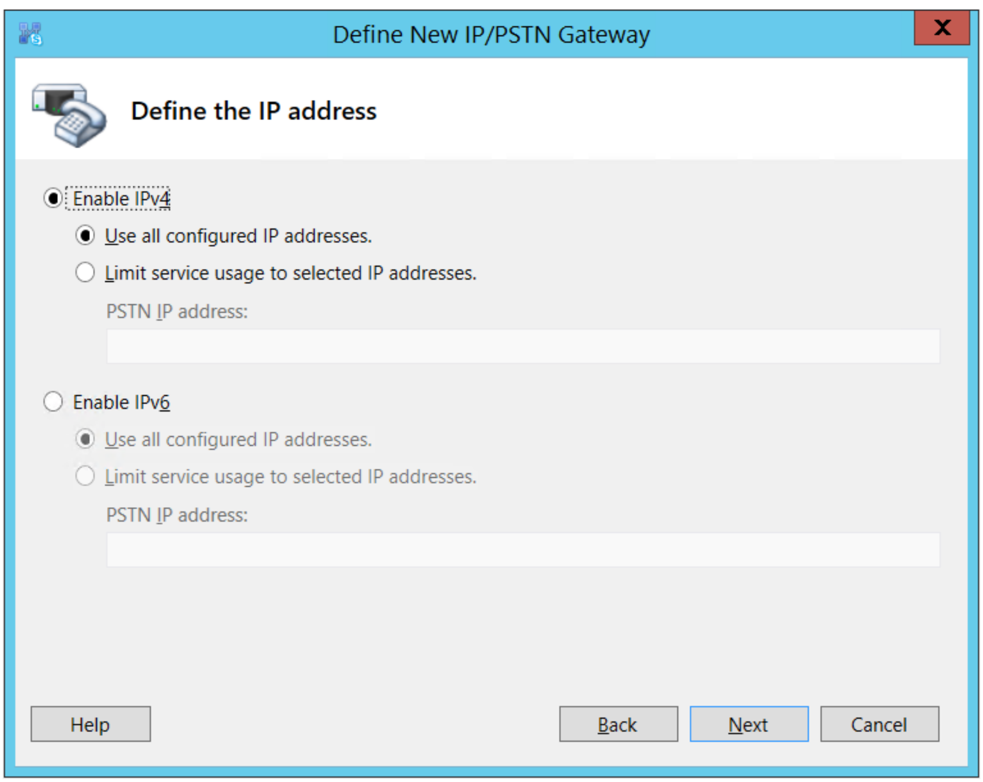


2. To define the **PSTN gateway**, expand **Shared Components** and right-click the **PSTN gateway**.

3. Click **New IP/PSTN Gateway**. The **Define the PSTN Gateway FQDN** dialog box appears.



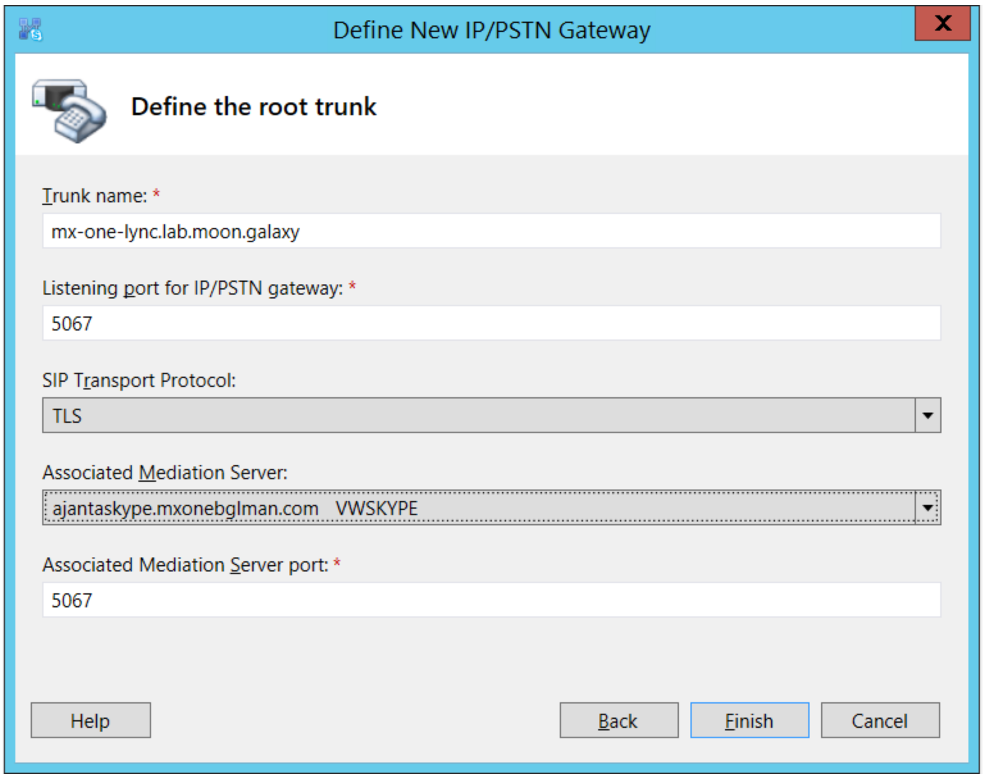
4. Enter the FQDN or the IP address: specify the MX-ONE IP Address or FQDN and click **Next**.
5. Define the IP address: in this example, the default is retained. Click **Next**.



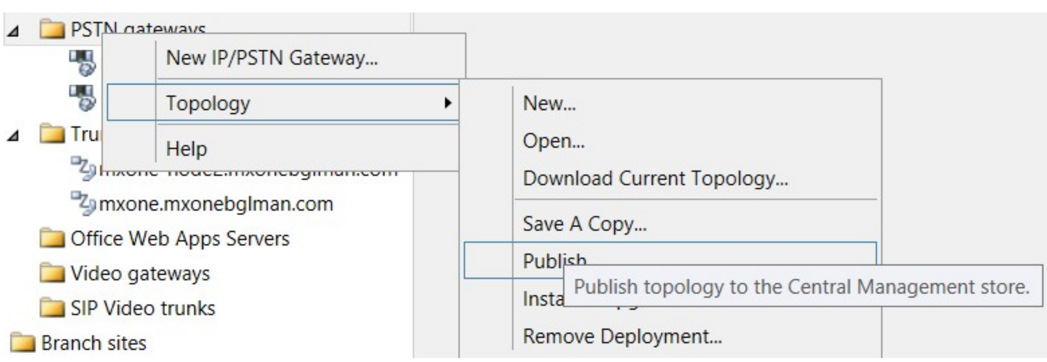
6. **Define the root trunk**:

- **Trunk name**: FQDN (MX-ONE FQDN)
- **Listening port for IP/PSTN gateway**: 5061 (MX-ONE SIP TCP port)
- **SIP Transport Protocol**: TCP
- **Associated Mediation Server**: lync-2019-se.moon.galaxy
- **Associated Mediation Server port**: 5067 (default)

7. Click **Next**.



8. Publish the **Topology**



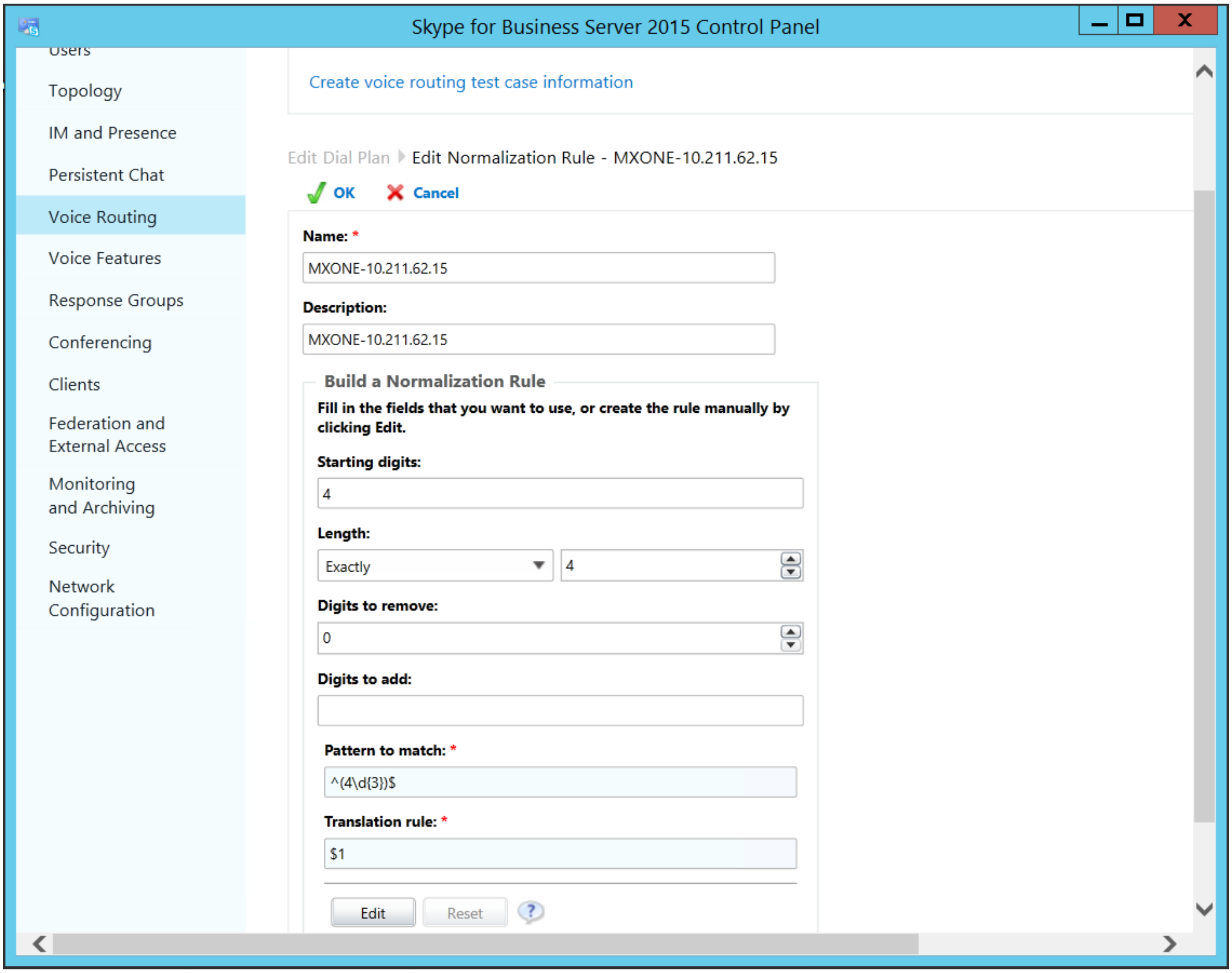
Define Dial Plan and Voice Policy

Define the ***Define a Dial Plan*** and the ***Define Voice Policy***as explained previously in this guide.

Define Trunk Configuration

To assign the MX-ONE gateway to a site or a pool trunk, and follow these steps:

1. Click **Voice Routing**, and then click **Trunk Configuration**.
2. Click **New** and choose the type of trunk that is applicable for your company setup, site trunk, or pool trunk.
3. Select **Enable media bypass**.



4. Keep the default Encryption support level, which in this case is **Required**.

Now that the setup is concluded, assign users with the policy created previously and test the integration making calls between the systems.

Load Balancing and Failover Setup

Load Balancing

Mitel MX-ONE 5.0 and later versions support load balancing setup when connected with more than one Mediation Server. In such scenario, the Microsoft DNS Load Balancing functionality can be used.

MX-ONE 5.0 and later versions support DNS SRV and multiple A-record query where a list with multiple entries can be used. When properly configured, MX-ONE will attempt to send an INVITE to the entries in the list until the call is successful. No answer or 503 Service Unavailable from one entry will trigger MX-ONE to try the next entry.

For more details, see MX-ONE `SIP Route` command description in CPI or sip_route –help, parameter remote port.

Failover

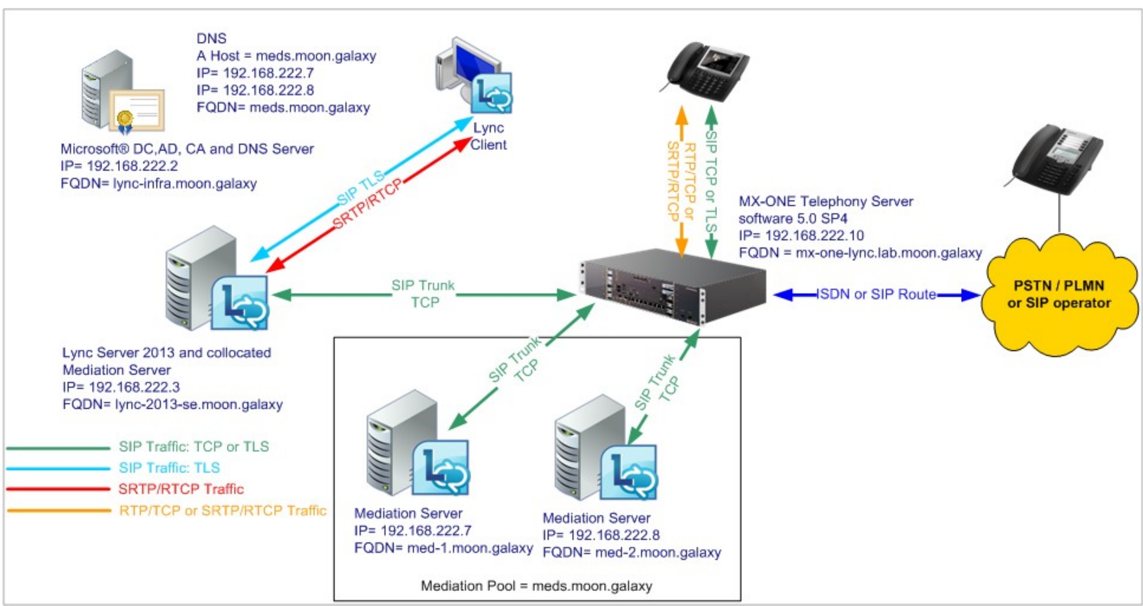
The failover feature also uses the Microsoft DNS Load Balancing functionality. When integrating MX-ONE and Mediation Server, the same configuration is valid for both failover and load balancing.

In a scenario, where two Mediation servers are used and if one of the servers is unavailable, then the first call will be attempted to set up to the first server, but it will be redirected after a few seconds and answered; and all subsequent calls will be redirected and answered in the second Mediation Server.

The reason it takes some seconds before getting an answer from the second server, is that after the INVITE is sent to the first server, the system waits four seconds for an answer, and if no answer is received, the host is grey-listed for 32 seconds and an INVITE is sent to the second server after this.

For additional details, see the MX-ONE `SIP Route` command description in CPI or sip_route – help, parameter remote port.

The following is a description of the setup that was verified in Mitel´s lab.



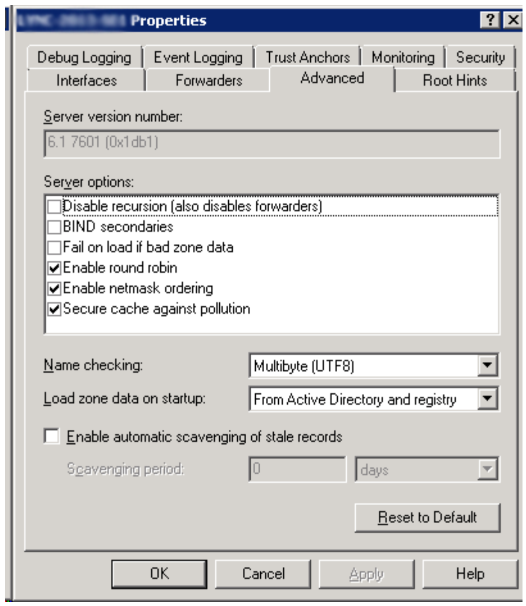
For this scenario, two standalone Mediation servers are used. In the MX-ONE side, only one MX-ONE Service Node is used, and it is configured with the Mediation Pool entry.

DNS Setup

Microsoft DNS needs to be configured to support Round Robin as described in the TechNet article "Configure DNS for Load Balancing". Follow the link and see the item "To enable round robin for Windows Server".

http://technet.microsoft.com/en-us/library/gg398251.aspx

The following figure shows the setup when Round Robin option is enabled.



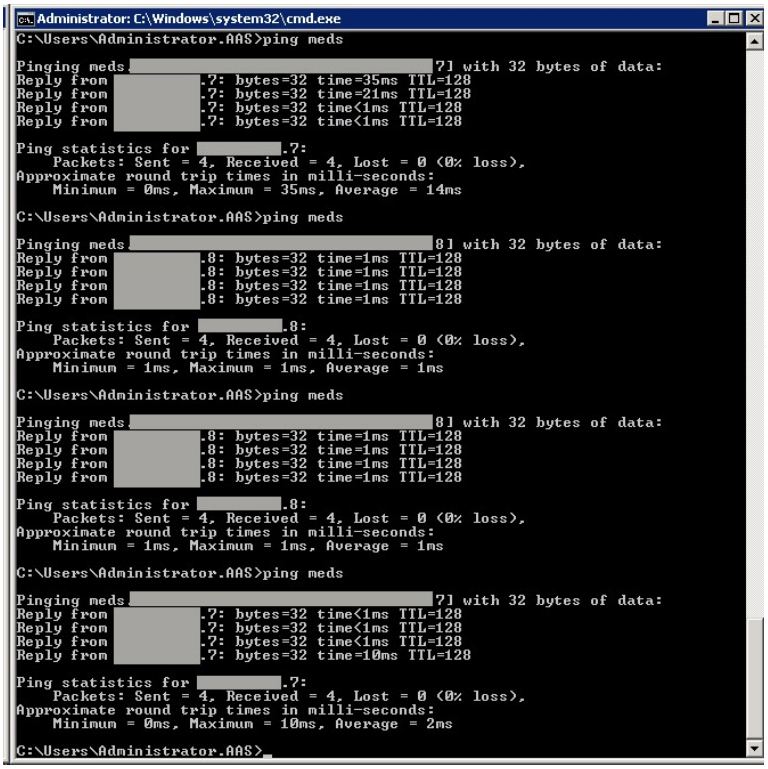
DNS Multiple A record setup – Mediation Servers

To set up DNS Host (A) records for the two Mediation servers, the following must be configured. In the DNS Manager Tool, create the entries as shown in the following table.

NOTE: For more information about creating the DNS Host A records, refer to http://technet.microsoft.com/en-us/library/gg398593.

FQDN	TYPE	IP ADDRESS
med.moon.galaxy	Host (A)	192.168.222.7
med.moon.galaxy	Host (A)	192.168.222.8

To test your configuration, use the command `ping` to check the setup.



MX-ONE Direct SIP with Load Balancing and Failover Setup - TCP

The following setup needs to be done in MX-ONE for configuring Direct SIP with load balancing and failover setup. Note that only Route definitions are shown.

NOTE: MX-ONE FQDN needs to be properly defined in the DNS Server.

1. Use the following command to view more details regarding the Profile Lync_TCP:
   `sip_route -print -profile Lync_TCP`
2. Define SIP Route category:

   RO-CAI:ROU=97,SEL=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4,SERV=3100 0000 01,BCAP=00110;
3. Define SIP Route data:

   RODAI:ROU=97,TYPE=TL66,VARC=00000000,VARI=00000000, VARO=00000000;
4. Define SIP trunk data specific:

   sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;
5. Verify the configuration:

   sip_route -print –route 97 -short
6. Define the SIP Route equipment initiate:

   ROEQI:ROU=97,TRU=1-1;
7. Define external destination SIP Route data:

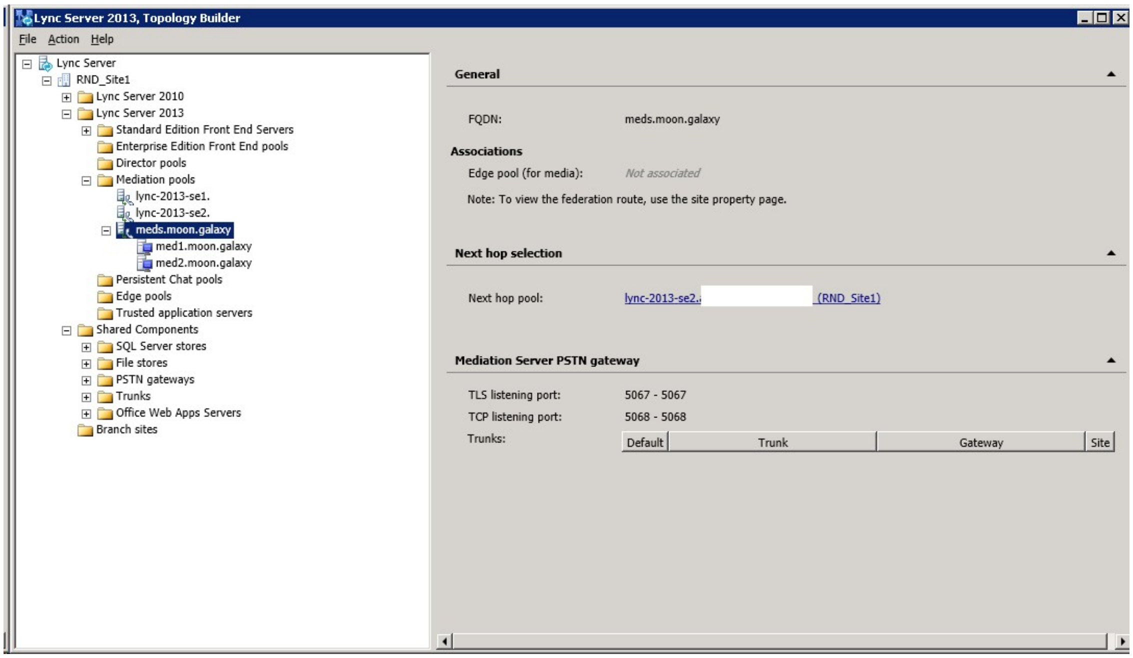
RODDI:ROU=97,DEST=97,ADC=0005000000000250000001010000,SRT=3;

Lync Configuration with Load Balancing and Failover Setup – TCP

Define a Mediation poll in the Skype for Business Server 2019 Topology Builder.

In the test validation, a Mediation poll named meds.moon.galaxy was created with two standalone Mediation servers.

Mediation Pool FQDN=meds.moon.galaxy Mediation Server 1 FQDN= med-1.moon.galaxy Mediation Server 2 FQDN= med-2.moon.galaxy



To set up the PSTN gateways, refer the Skype for Business Server 2019 configuration - TCP.

Execute calls between MX-ONE and Microsoft Lync and check that the calls are distributed between the systems.

MX-ONE Direct SIP with Load Balancing and Failover Setup - TLS

The following setup needs to be done in MX-ONE in order to configure Direct SIP with load balancing and failover setup, please note that only Route definitions are showed.

NOTE: MX-ONE FQDN needs to be properly defined in the DNS Server.

1. Use the following command to check more details regarding SIP Profile Lync_TLS sip_route -print -profile Lync_TLS
2. Define SIP Route category:

   ROCAI:ROU=96,SEL=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=00110;
3. Define SIP Route data:

   RODAI: ROU=96,TYPE=TL66,VARC=00000000,VARI=00000000, VARO=00000000;
4. Define SIP trunk data specific:

sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;

5. Verify your configuration:

   sip_route -print –route 96 -short

6. Define the SIP Route equipment initiate:

   ROEQI:ROU=96,TRU=1-1;

7. Define external destination SIP Route data:

   RODDI: ROU=96,DEST=96,ADC=0005000000000250000001010000,SRT=3;

Import the Certificate to MX-ONE Service Node

Import the server certificate mx-one-certificate.pfx to MX-ONE Service Node. On the access Server, for example, MX-ONE Service Node 1 runs the following command:

1. Install the certificate in the MX-ONE Service Node 1: mxone_certificate, and select the certificate mx-one-certificate.pfx
2. Enable Media Encryption in the route: media_encryption_enable –type route

Lync Configuration with Load Balancing and Failover Setup – TLS

Define a Mediation poll in the Skype for Business Server 2019 Topology Builder.

In the test validation, a Mediation poll named meds.moon.galaxy was created with two standalone Mediation servers.

Mediation Pool FQDN=meds.moon.galaxy Mediation Server 1 FQDN= med-1.moon.galaxy Mediation Server 2 FQDN= med-2.moon.galaxy

To set up the PSTN gateways, refer the Lync configuration with security and Media Bypass setup section.

Execute calls between MX-ONE and Microsoft Lync and check that the calls are distributed between the systems.

Integration Notes

The latest software and firmware versions of MX-ONE components must be used.

NOTE: Mitel recommends that complex scenarios shall be validated in the partner labs before to customer deployment.

References

Always check the latest documentation. The links below are the ones available for reference. Mitel CPI Documentation – Mitel MX-ONE 5.0 SP4 or a later version.

Skype for Business Server Deploying Enterprise Voice

Enable Users for Enterprise Voice

Revision History

DOCUMENT VERSION	COMMENTT	DATE
A	First release	2015-11-19
B	Minor corrections	2014-03-28
C	Updated with Mitel template	2015-06-08
D	Updated in 4.2.3.7, cert_install_local replaced by mxone_certificate. MX-ONE version information also corrected.	2015-10-27
D3	Spelling correction	2017-04-05
D4	2013 old screens replaced with 2015 screens	2019-04-24
D5	Server 2015 is changed to server 2019	2019-09-10

Introduction

The MiVoice MX-ONE communication system is based on an open software and hardware environment, using standard servers with a Linux SUSE operating system. This open standards approach enables Mitel to offer our customers a choice and with this in mind we have worked together with Microsoft to ensure that MiVoice MX-ONE can be integrated with the latest Microsoft UC products.

General

MX-ONE 7.x version can interwork with third party UC products using standards-based protocols, such as SIP and CSTA V3/XML. Note however, that the configuration described in this version of the document, is valid for MX-ONE 6.0 SP2 or later releases.

Integration of MX-ONE 6.1 (and 6.0 and 5.0 SP4 or later) can be done with the Microsoft Exchange Server 2013 Unified Messaging (UM) as a complementary solution providing end user services like voice mail, Unified Messaging and auto attendant as well as system functionalities such as load balancing and fault tolerance.

Microsoft Partner Program has certified the integration between MX-ONE 5.0 SP4 and Microsoft Exchange Server 2013 Unified Messaging (UM) via a Direct SIP connection.

Scope of this Document

The intent of this guide is to describe the basic integration between the MiVoice MX-ONE and Microsoft Exchange Server 2013 Unified Messaging as well as describe the configuration needed and what features are available after the integration. The following sections describe the solution integration that has been certified through the Microsoft partner program and also the tests performed in Mitel´s laboratory.

For a more technical description on how this integration is set-up, as well as tested features, we refer to the relevant CPI documentation for MX-ONE or please, go to the Microsoft Exchange Server 2013 product websites.

	Note! Always check the latest products documentation.

Solution Description

The integration of MX-ONE 7.x and Microsoft Exchange Server 2013 Unified Messaging described in this guide is achieved via Direct SIP.

Direct SIP that is specified by Microsoft means that a SIP trunk is used to connect MX-ONE 7.x and Microsoft Exchange Server 2013 Unified Messaging. Additionally, MX-ONE can be configured with TLS and SRTP when integrated with Exchange 2013 UM to provide security in the transport between the systems as well as load balancing and failover functionalities.

MiVoice MX-ONE 7.x Integration with Microsoft Exchange Server 2013 UM

The solution diagram below shows how MX-ONE is connected with Exchange 2013 UM.

In the validated scenario both Client Access and Mailbox role run in the same Exchange Server.

	Note! Microsoft Exchange Server 2013 architecture is different than the architecture in Exchange Server 2010, read Microsoft document “Voice Architecture Changes for more information.

http://technet.microsoft.com/en-us/library/jj150516(v=exchg.150).aspx

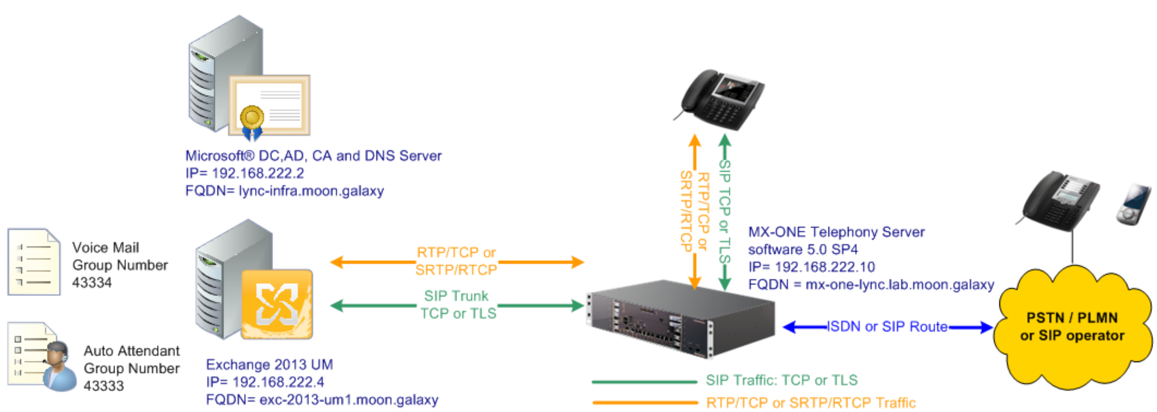


Figure 1 - MX-ONE 7.x integration with Microsoft Exchange Server 2013 UM

As described in Microsoft´s documentation: “In the new model, the Client Access server running the Microsoft Exchange Unified Messaging Call Router service redirects Session Initialization Protocol (SIP) traffic that’s generated from an incoming call to a Mailbox server. Then a media (Realtime Transport

Protocol (RTP) or secure RTP (SRTP)) channel is established from the VoIP gateway or IP Private Branch eXchange (PBX) to the Mailbox server that hosts the user's mailbox."

In short, the Direct SIP integration works in the following way: When MX-ONE is configured to use TCP as transport, it calls to Microsoft Exchange 2013 UM by sending a SIP INVITE message to the 5060 port of Exchange Server. Then, Exchange Server sends 302 (Moved Temporarily) back to MX-ONE asking to send the INVITE on a different port (TCP: for example, 5065 or 5067). After the MX-ONE sends the INVITE to the new port, the call setup is executed and the call is established.

MX-ONE integrated with Microsoft Exchange Server 2013 Unified Messaging delivers the following end user features:

- Voice mail
- Auto Attendant
- Message waiting indication for MX-ONE terminals
- Outlook voice access

Licenses

The licenses needed are:

MiVoice MX-ONE Licenses

The MiVoice MX-ONE licenses needed for this integration are:

- SIP trunk licenses. At a minimum there is the need for one SIP trunk license (SIP route) per Microsoft Exchange 2013 UM server.
- SIP trunk channel licenses (port licenses in proportion to the maximum number of simultaneous Voice Mail messages that shall be supported).
- License for private network services is also required for the SIP route.

Note! Actual quantity of licenses will depend on the customer installation.

- An optional VoIP Encryption license is required if security (TLS/SRTP) is used.

Please, always check with your Mitel partner that your system has the correct licenses, before beginning the integration deployment.

Microsoft Exchange 2013 UM Licenses

Microsoft licenses needed for this integration are not included as part of the scope of this guide. Please, contact Microsoft or a qualified Microsoft partner to obtain the proper license requirements for each component of the Microsoft Exchange 2013 UM solution.

MX-ONE Integration with Exchange 2013 UM using TCP

Prerequisites

MiVoice MX-ONE Prerequisites

Main components

MiVoice MX-ONE 6.0 SP2 (or later version) with the proper licenses.

At least the following MX-ONE components are required:

- MiVoice MX-ONE communications system

MX-ONE Service Node

MX-ONE Service Node 6.0 SP2 or later version

Supported media gateways with the latest compatible firmware with MX-ONE 6.0 SP2 or later version

MX-ONE Classic - 7U 19-inch chassis, using MGU boards or

MX-ONE Lite - 3U 19-inch chassis, using MGU board

MX-ONE 1U 19-inch chassis, using MGU board

MX-ONE Media Server (soft media gateway)

The following shall be configured:

- Trunk between MX-ONE and Exchange UM - SIP route.
- Message Waiting Indicator configuration in the system and in the phones that will use the service.
- Call list or Diversion for IP phones. These features are used to forward the call to the voice mail in case of no answer or busy.

The following MX-ONE type of devices can be used with Exchange 2013 UM:

- SIP – Mitel 6700i/6800i family or any device supporting baseline SIP. As the Exchange Server also supports SIP with Direct Media, MX-ONE gateway resources would not be needed for SIP devices. But, in order to guarantee interoperability with any 3rd party SIP terminal, the SIP route to Exchange UM can be setup as “forced gateway”. The effect is that SIP calls to the Exchange UM server will always transit via the MX-ONE media gateway (MGU) for a call setup and media.
- Non SIP – All non-SIP devices calling into the Exchange UM server will transit via the MX-ONE Media GW (MGU based) for call setup and media. The following is the list of supported devices:

H.323 -MiVoice 4400 IP phones and Mitel 7400 IP phones

Digital phones: MiVoice 4200 series digital phones

Analog phones: MiVoice 4100 series analog phones

Mitel Cordless Phones: DT690, DT390, DT412, DT422, DT432

Mobiles devices (no MWI functionality) using MX-ONE’s Mobile extension service

External callers coming in via the MX-ONE public access, regardless of the type of terminal or network connection (SIP or TDM)

Microsoft Exchange 2013 UM Prerequisites

This guide does not cover the Exchange 2013 UM installation, so our recommendation is that Microsoft Exchange 2013 UM shall be installed by a trained Microsoft engineer.

Before you start to install Microsoft Exchange 2013 Unified Messaging, please read the Microsoft Exchange 2013 documentation for a better understanding of the solution requirements. The documentation can be found in the following links:

- Microsoft Exchange 2013 documentation
- http://technet.microsoft.com/en-us/library/bb124558(v=exchg.150).aspx
- Microsoft Exchange 2013 Unified Messaging
- http://technet.microsoft.com/en-us/library/jj150478(v=exchg.150).aspx

Configuration

In this configuration example, we have used the following information:

Direct SIP connection using TCP as transport

MX-ONE

- IP address: 192.168.222.10
- FQDN: mx-one-lync.lab.moon.galaxy
- Numbering Plan: 5 digits
- Access numbers (external destinations) for Voice Mail and Auto Attendant: 43334 and 43333 (could be the same number for VM and attendant, if wanted, but here different numbers are used).
- Route access codes: 43333, 43334
- Users IP extensions: 27000, 27001 and 27010.

Exchange UM

- IPv4: 192.168.222.4
- FQDN: exc-2013-um1.moon.galaxy
- Voice Mail Pilot identifier: 43334
- Auto Attendant: 43333

MiVoice MX-ONE Configuration

Voice Mail and Auto Attendant Numbers

The Voice Mail and the Auto Attendant numbers need to be initiated. In this example, the service number 43334 is used for Voice Mail and the service number 43333 is used for Auto Attendant.

Number Initiation:
number_initiate-numbertypeED -number 43333
number_initiate -numbertype ED -number 43334

Creating SIP trunk

The following commands shall be executed in MX-ONE to configure a SIP Trunk.

Basic Setup:

rocai:rou=55,sel=7110000000000010,sig=0111110000A0,traf=03151515,trm=4,serv=3110000001,bcap=000100; Wanted options for the SIP route are: Forcedgateway, and 9 sec timeout for 100 Trying. Since SIP route profiles will be used, the var-parameter settings do not matter, but we still must enter RODAI, so we will set all var parameters 0, but the profile shall set Forced gateway and 9 s timeout.
rodai:rou=55,type=TL66,vari=00000000,varc=00000000,varo=00000000;

Please note that Message Waiting Indication number needs to be defined in the SIP route via mwinumber parameter as shown in the example.

SIP Route Setting:
sip_route-set -route 55 -profileExchangeUM_TCP-uristring0sip:?@192.168.222.4-match 192.168.222.4 -accept REMOTE_IP -codecs PCMA,PCMU -mwinumber43334 #mwinumberis the Message Waiting Indication number

Route equipment and destination data:
#Node 1 (as in node x, as in TRU=x-1) for MX-ONE SIP access, in this case the IP address 192.168.222.10 is configured in the MX-ONE Service Node 1. roeqi:rou=55,tru=1-1&&1-xx;

Define external destinations to the SIP route 55
roddi:rou=55,dest=43333,adc=0005000000000250000001010000,SRT=1;
roddi:rou=55,dest=43334,adc=0005000000000250000001010000,SRT=1;

User configuration to forward to Voice Mail

Any third party terminal registered in MX-ONE may subscribe on Message Waiting Indicator (MWI) according to RFC 3842.

The commands below enable a user to forward calls to Exchange Server voice mail.

The example shows how calls will be forwarded to Exchange 2013 UM Voice Mail number 43334 if a call is made to extension 27000 on no answer.

Call List Setup:
call_list-i-d 27000 --dest-number 27000 --position 1 --busy-position 2
call_list-i-d 27000 --dest-number 43334 --position 2 --ird-bypass true

The extensions can also use Call Diversion instead of the Call List.

Other Extension User configuration related to Voice Mail

For H.323 Dialog terminals: If there is no fixed key for Voice Mail on the terminal, a function key, ‘Message Waiting’ must be enabled in order to enable speed dial. The key is enabled in a common phone configuration file (for example d42x02-config.txt).

For SIP 6700i terminal family: In the common phone configuration file, aastra.cfg, set “sip line1 vmail: 43334” to enable speed dial to voice mail. Similarly for 6800i terminals.

Microsoft Exchange 2013 UM

In order to setup the Exchange 2013 UM, please check Microsoft´s documentation:

Deploy Exchange 2013 UM

http://technet.microsoft.com/en-us/library/jj673564(v=exchg.150).aspx

After the installation of the Exchange 2013 UM roles, the following steps need to be executed to create the integration between MX-ONE and Exchange 2013 UM.

UM Dial Plan

A "UM Dial Plan" needs to be created in the Exchange UM.

Before you create a UM dial plan, please read the Microsoft's document, UM Dial Plans.

http://technet.microsoft.com/en-us/library/bb125151(v=exchg.150).aspx

To create a New UM dial plan, please follow the step 1 in Microsoft's document, Create a UM dial plan.

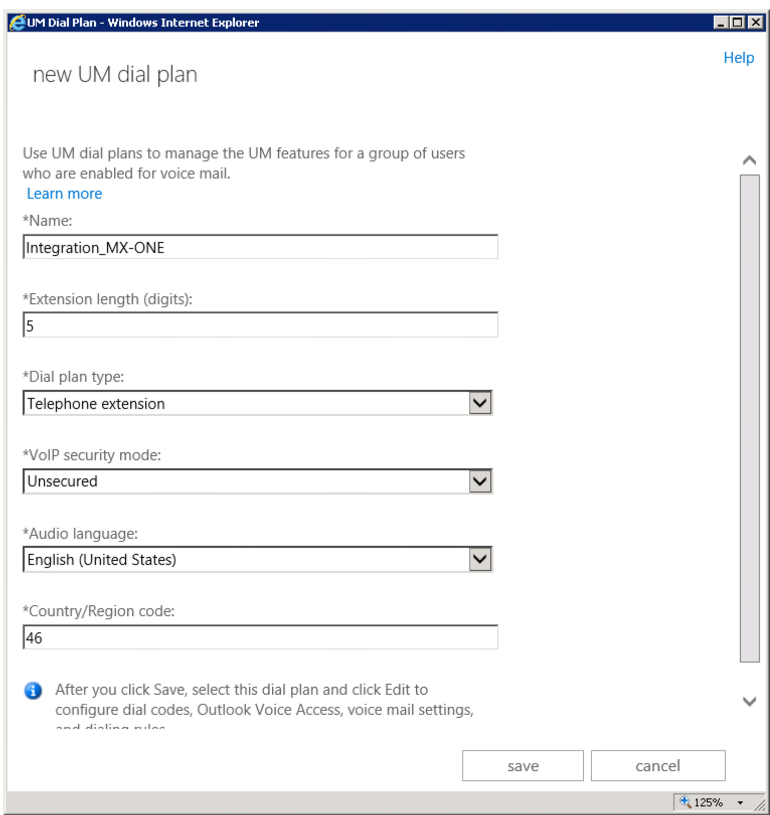
http://technet.microsoft.com/en-us/library/jj673564(v=exchg.150).aspx

Example:

- UM Dial Plan: Integration_MX-ONE
- Number of digits in extensions numbers: 5 - It needs to match the number of digits of the MX-ONE extensions.
- VoIP Security: Unsecured. In this example TCP is used.

The screen below shows the required configuration for the example.

•



UM IP gateway

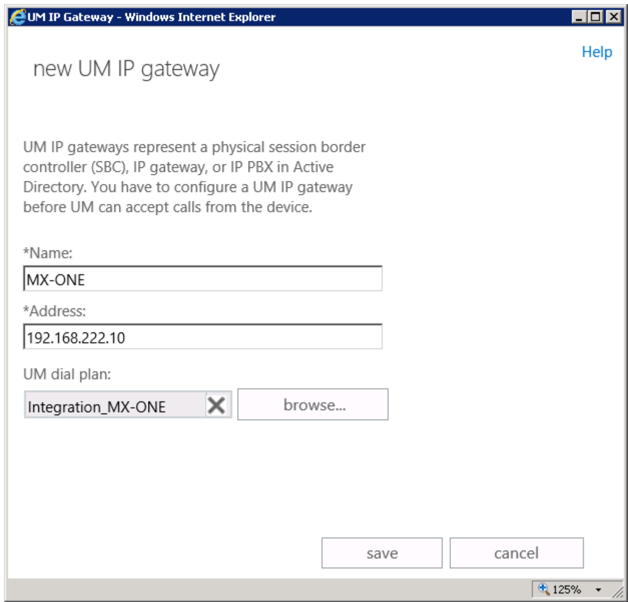
A UM IP gateway needs to be created in the Exchange UM.

To create a UM IP gateway, follow the step 2 in Microsoft's document:

http://technet.microsoft.com/en-us/library/jj673564(v=exchg.150).aspx

Example:

- Name of the gateway: MX-ONE
- IP address: 192.168.222.10
- Dial Plan: It is the same one created previously.



UM Hunt Group

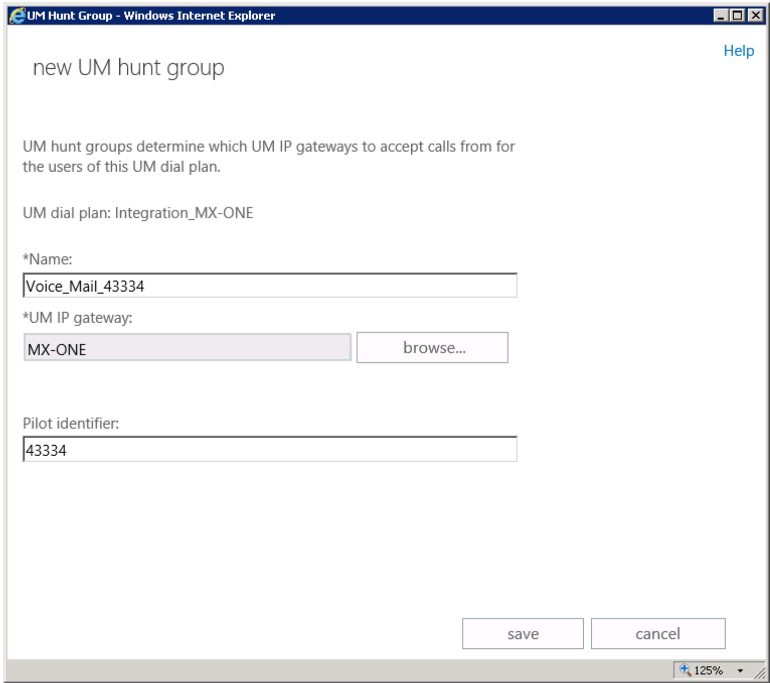
A Hunt group shall be created to the voice mail.

To create a UM Hunt Group, follow the steps in Microsoft's document:

https://technet.microsoft.com/en-us/library/aa997679.aspx

Example:

- Associated UM IP Gateway: MX-ONE
- Name: Voice_Mail_43334
- Dial Plan: Integration_MX-ONE
- Pilot identifier: 43334. It must be the same number that was previously created in MX-ONE.



UM Mailbox Policies

A new UM mailbox policy can be created or the default policy can be used. Please, follow step 4 in Microsoft's document:

http://technet.microsoft.com/en-us/library/jj673564(v=exchg.150).aspx

UM Auto Attendant

To setup the Exchange 2013 UM Auto Attendant, please follow the steps below:

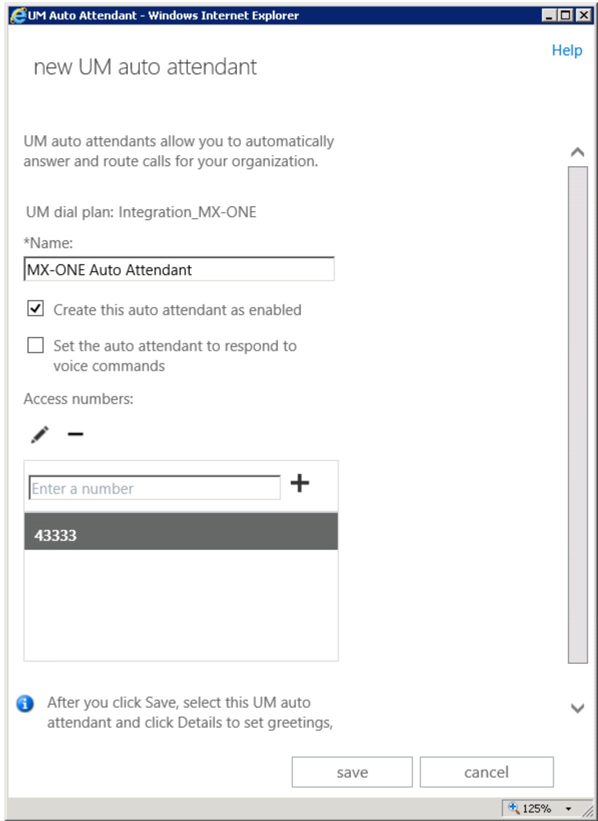
Create an UM Auto Attendant

To create an UM Auto Attendant, please follow the step 5 in Microsoft's document:

http://technet.microsoft.com/en-us/library/jj673564(v=exchg.150).aspx

Example:

- Name: MX-ONE Auto Attendant
- Dial Plan: Integration_MX-ONE
- Pilot identifier: 43333. It needs to be the same number that was previously created in MX-ONE.



Enable the Unified Messaging

To enable Voice Mail for a user follow Microsoft´s document:

Enable a User for Voice Mail

http://technet.microsoft.com/en-us/library/bb124147(v=exchg.150).aspx

MiVoice MX-ONE Integration with Exchange 2013 UM Using TLS

Prerequisites

MiVoice MX-ONE Prerequisites

Main components

MiVoice MX-ONE 6.0 SP2 or later version with the proper licenses.

At least the following MX-ONE components are required:

- MiVoice MX-ONE communications system

MX-ONE Service Node

MX-ONE Service Node 6.0 SP2 or later version

Supported media gateways with the latest compatible firmware with MX-ONE 6.0 SP2 or later version

MX-ONE Classic - 7U 19-inch chassis, using MGU boards or

MX-ONE Lite - 3U 19-inch chassis, using MGU board

MX-ONE 1U 19-inch chassis, using MGU board

MX-ONE Media Server (soft media gateway)

Licenses

All licenses described in the item 3.1 MX-ONE Licenses

VoIP Encryption license is required (TLS/SRTP) as TLS and SRTP will be used.

The following shall be configured:

- Trunk between MX-ONE and Exchange UM – SIP route configured with TLS.
- Two access numbers (external destinations) to be used as Pilot numbers (groups) in Exchange UM.
- Message Waiting Indicator configuration in the system and in the phones that will use the service.
- Call list or Diversion for IP phones. These features are used to forward the call to the voice mail in case of no answer or busy.

Microsoft Exchange 2013 UM Prerequisites

This guide does not cover the Exchange 2013 UM installation. Our recommendation is that Microsoft Exchange 2013 UM shall be installed by a trained Microsoft engineer.

Before you start to install Microsoft Exchange 2013 Unified Messaging server role, please read the Microsoft Exchange 2013 documentation for a better understanding of the solution requirements, the documentation can be found in the following links:

- Microsoft Exchange 2013 documentation

http://technet.microsoft.com/en-us/library/bb124558(v=exchg.150).aspx

- Microsoft Exchange 2013 Unified Messaging

http://technet.microsoft.com/en-us/library/jj150478(v=exchg.150).aspx

Configuration

In this configuration example, we used the following:

Direct SIP connection using TLS as transport

MX-ONE

- IP address: 192.168.222.10
- FQDN: mx-one-lync.lab.moon.galaxy
- Numbering Plan: 5 digits
- Access numbers for Voice Mail and Auto Attendant: 43334 for VM and 43333 for attendant.
- Route access code: 043
- Users IP extensions: 27000, 27001 and 27010.

Exchange UM

- IPv4: 192.168.222.4
- FQDN: exc-2013-um1.moon.galaxy
- Voice Mail Pilot identifier, Hunt Group: 43334
- Auto Attendant: 43333

Certificate:

To use TLS between MX-ONE and Exchange 2013 UM a certificate must be created.

The common Microsoft Enterprise CA used for signing server certificates for Mediation Server and Exchange 2013 UM is assumed to be used to create a server certificate for MX-ONE as well.

A server certificate is signed to the FQDN (Fully Qualified Domain Name) of MX-ONE Service Node.

Create a Certificate

When using security, an appropriate certificate needs to be installed in MX-ONE as well as the encryption licenses. Please, check Certificate Management on MX-ONE CPI documentation in case you need more details regarding certificates.

Import the certificate to MiVoice MX-ONE Service Node

Import the server certificate, in the example, mx-one-lync.lab.moon.galaxy.pfx to MX-ONE Service Node accessing the Exchange 2013 UM.

On the access Server, for example, MX-ONE Service Node 1 run the command:

Install certificate in MX-ONE Service Node
mxone_certificate, with the certificate mx-one-lync.lab.moon.galaxy.pfx

MiVoice MX-ONE Configuration

Creating SIP trunk with TLS

The following commands shall be executed in MX-ONE to configure a SIP Trunk with TLS, the others commands are the same as in a TCP configuration.

SIP Route settings for TLS
sip_route -set -route 55 -profile ExchangeUM_TLS_SRTP -uristring0 sip:?@192.168.222.4 -match 192.168.222.4 -accept REMOTE_IP -codecs PCMA,PCMU -mwinumber 43334 #mwinumberis the Message Waiting Indication number

	Note! -accept REMOTE_IP will match the IP address sent in the IPv4 source IP header.
Enable Media Encryption in the route:	
media_encryption_enable-type route	

Microsoft Exchange 2013 UM

In order to setup Exchange 2013 UM to use TLS, please follow Microsoft´s documentation.

http://technet.microsoft.com/en-us/library/jj150478(v=exchg.150).aspx

Load Balancing and Failover Between MiVoice MX-ONE and Two Exchange Servers

Load Balancing

MiVoice MX-ONE 7.x supports load balancing when connected with more than one Exchange Server UM. To be able to use such a scenario, the Microsoft DNS Load Balancing functionality is used.

MX-ONE 7.x supports DNS SRV and multiple A record query where a list with multiple entries can be used. When proper configured, MX-ONE will attempt to send INVITE to the entries in the list until the call is successful. No answer or 503 Service Unavailable will trigger MX-ONE to try the next entry.

For more details, check MX-ONE SIP Route command description in CPI or sip_route –help, parameter remoteport.

Failover

The failover functionality also requires Microsoft DNS Load Balancing functionality. When integrating MX-ONE and Exchange UM, the same configuration is valid for both failover and load balancing.

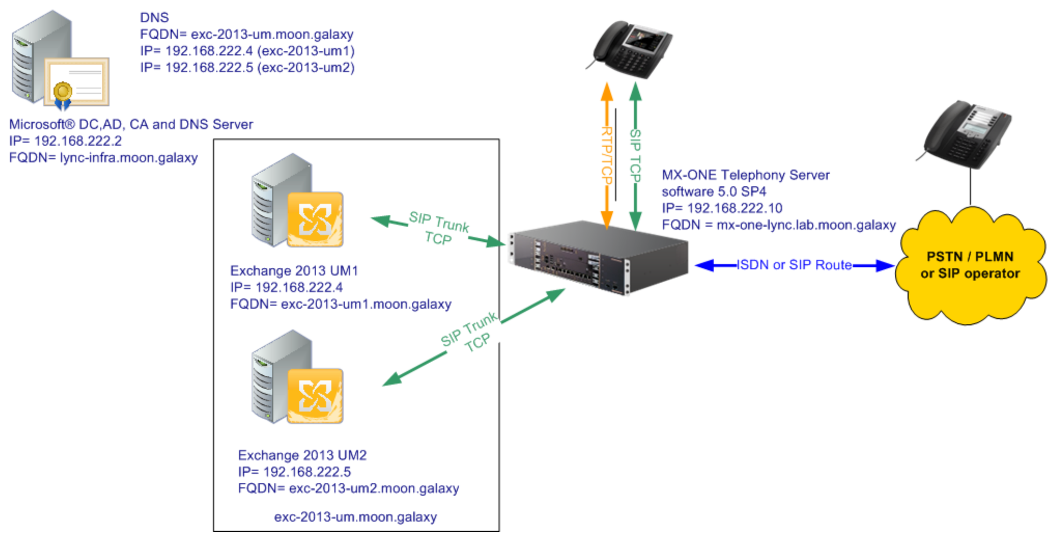
In a scenario where 2 Exchange UM servers are used and one of the servers is unavailable, the first call will be attempted to set up to the first server, but it will be redirected after a few seconds and answered. Then subsequent calls will be redirected and answered in the second Exchange UM.

The reason why it takes some seconds before getting answer is that the INVITE is sent to the first server, then the system waits 4 seconds for an answer. If no answer is received, the host is grey-listed for 32 seconds and an INVITE is sent to the second server.

For more details, check MX-ONE SIP Route command description in the CPI or sip_route –help, parameter remoteport.

Load Balancing and Failover Scenario

The figure below shows the validated setup:



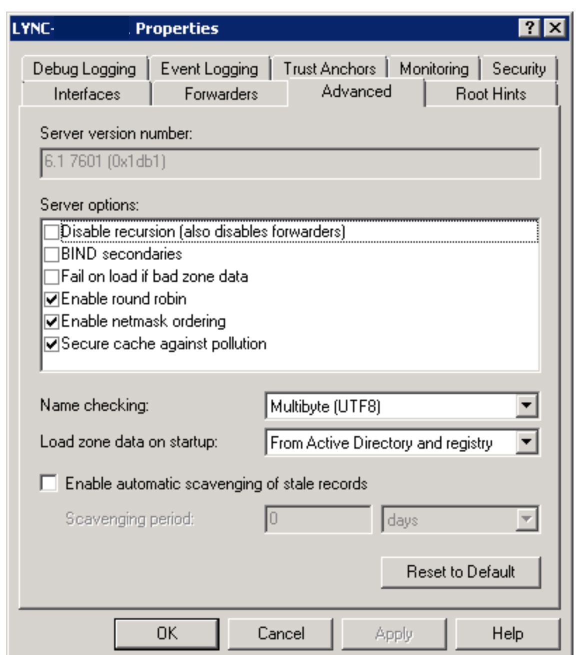
Configuration

DNS Setup

Microsoft environment needs to be configured to support Round Robin as described in the TechNet article "Configure DNS for Load Balancing". Please, see the link below, item "To enable round robin for Windows Server".

http://technet.microsoft.com/en-us/library/gg398251.aspx

The figure below shows the Round Robin option enabled.



DNS SRV setup

Go to DNS Manager Tool and create a pool entry. After that, add a DNS SRV record to each Exchange UM Server that participates in the DNS Load Balancing. In the following example the FQDN pool name is exc-2013-um.

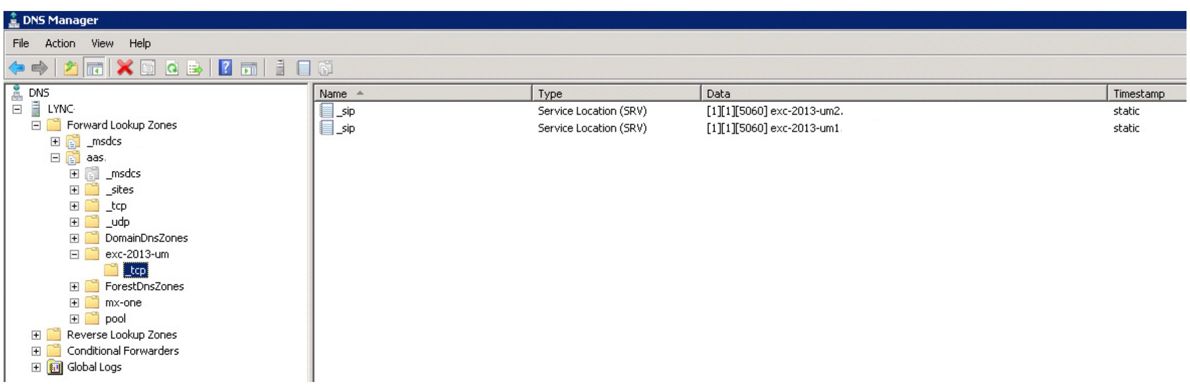
The values below needs to be configured in the DNS SRV record for each Exchange UM that is part of the pool.

DNS SRV	Values
Service:	_sip
Protocol:	_tcp
Priority:	1
Weight:	1
Port Number:	5060
Host offering this service	exc-2013-um1 exc-2013-um2

Please check the following Microsoft article for more details.

http://technet.microsoft.com/en-us/library/gg398680

The figure below shows the exc-2013-um pool after the SRV Records configuration:



Test DNS SRV record setup

Using the Windows command nslookup, test the configuration:

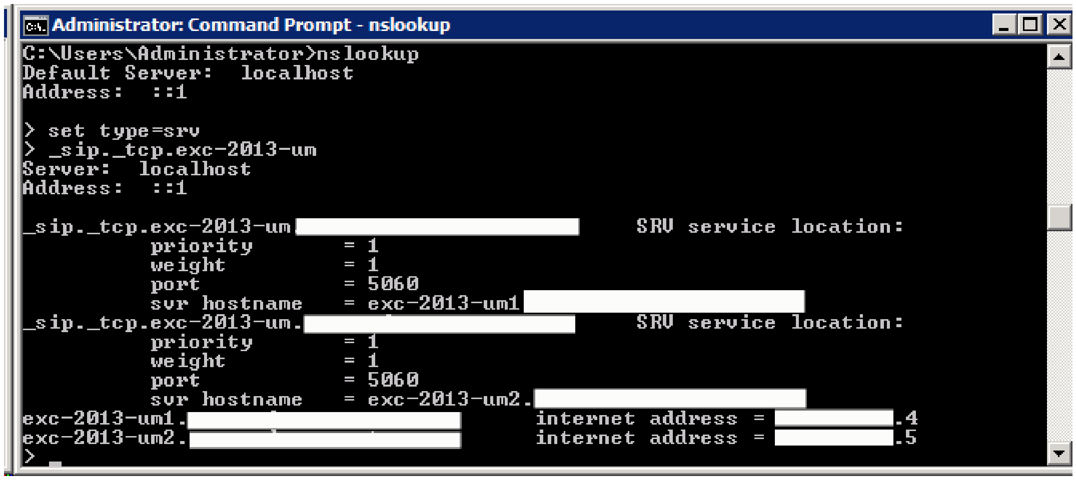
nslookup

set type=srv

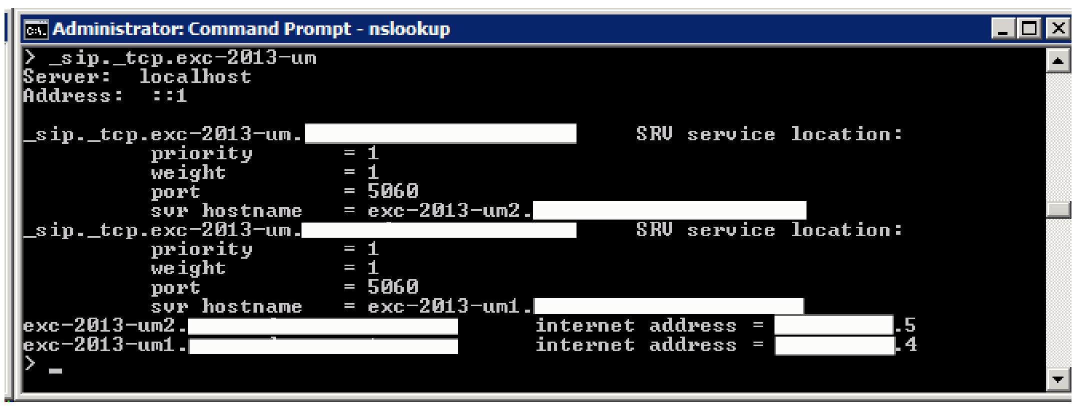
_sip._tcp.exc-2013-um

The expected result is presented in the 2 next screens. Please note the domain name and the IP addresses are just partially presented.

The first query the DNS replies with exc-2013-um1.



The second query the DNS replies with exc-2013-um2.



Creating MiVoice MX-ONE SIP trunk

The MX-ONE SIP Route Outbound setting needs to be configured with the FQDN pool name that is used to solve the Exchange UM Servers that are part of the “load balancing cluster”. Please, note that remote-port should be configured equal 0. This is needed by MX-ONE in order to use the DNS SRV option.

Outbound Setting:
sip_route-set -route 55 -uristring0 sip:?@exc-2013-um.moon.galaxy -remoteport0 -protocoltcp-codecs PCMA,PCMU -mwinumber43334 #mwinumberis the Message Waiting Indication number

Please note that Exchange 2013 UM IP addresses needs to be defined in the parameter match, as shown in the example.

Inbound Setting:
ip_route -set -route 55 -accept REMOTE_IP -match 192.168.222.4,192.168.222.5 # match = Exchange 2013 UM IP addresses

How to Test the Integration

To execute the integration test, the configuration in both sides shall be ready.

How to Test the Integration

Basic Tests

Dial the pilot number from a phone extension that is NOT enabled for Unified Messaging and logon to a user's mailbox.

Confirm hearing the prompt: "<Microsoft Exchange Earcon>. To access your mailbox, enter your extension…"

Navigate mailbox using the Voice User Interface (VUI).

Navigate mailbox using the Telephony User Interface (TUI).

Dial user extension and leave a voicemail.

Dial user extension and leave a voicemail from an internal extension.

Confirm that the Active Directory name of the calling party is displayed in the sender field of the voicemail message.

Dial user extension and leave a voicemail from an external phone.

Confirm that the correct phone number of the calling party is displayed in the sender field of the voicemail message.

Dial Auto Attendant (AA).

Dial the extension for the AA and confirm that the AA answers the call.

Call Transfer by Directory Search.

Call Transfer by Directory Search and have the called party answer.

Confirm that the correct called party answers the phone.

Call Transfer by Directory Search when the called party's phone is busy.

Confirm that the call is routed to the called party's voicemail.

Call Transfer by Directory Search when the called party does not answer.

Confirm that the call is routed to the called party's voicemail.

Setup an invalid extension number for a particular user.

Call Transfer by Directory Search to this user. Confirm that the number is reported as invalid.

Outlook Web Access (OWA) Play-On-Phone Feature.

Listen to voicemail using OWA's Play-On-Phone feature to a user's extension.

Listen to voicemail using OWA's Play-On-Phone feature to an external number.

Configure a button on the phone of a UM-enabled user to forward the user to the pilot number.

Press the voicemail button.

Confirm that you are sent to the prompt: “<Microsoft Exchange UM Earcon>. <User>. Please enter your pin and press the pound key.”

MWI.

Ensure that a UM-enabled user’s mailbox does not have any new voice mails.

Dial the user’s extension and leave a voicemail. Confirm that the MWI lamp on the phone lights up.

Mark the voice mail email as read in OWA. Confirm that the MWI lamp on the phone turns off.

Load balancing

Open the Wireshark tool and configure it to collect SIP packets.

Dial several times to the voice mail number from an SIP extension. Use the Wireshark tool to analyze the SIP packet in order to verify that the load balancing is working properly.

Failover

Disconnect the Ethernet cable of Exchange 2013 UM 1 to simulate a failure.

Dial several times to the voice mail number from an SIP extension. Check that the calls are answered in the Exchange 2013 UM 2.

Introduction

MiVoice MX-ONE, a complete IP-based communications system, has evolved from a voice centric system into a true multimedia communication system that can route and provide services to media sessions like video, instant messaging etc. It is the core component of the MX-ONE solution, which provides the necessary applications to offer true mobility and Unified Communications and Collaboration (UCC). MX-ONE (TS) is based on an open software and hardware environment, using standard servers with a LINUX SUSE operating system. MX-ONE Service Node focuses on enhanced SIP implementations to target our strategy regarding openness, cloud computing and video support. An example of MX-ONE openness is the fact that it can interwork with third party UC products using standards-based protocols, such as SIP and CSTA III (XML).

As part of this standards-based approach and in order to offer our customers a choice, we have worked together with Microsoft to ensure that MX-ONE can be integrated with the latest Microsoft Unified Communications products. MX-ONE is fully certified by the Microsoft Partner Program since Version 4.1 with Lync Server 2010 (Direct SIP integration) as well as MX-ONE 5.0 SP3 HF2 with Lync 2013 (Direct SIP integration) in order to ensure that customers have seamless experiences with setup, support, and use of MX-ONE with Microsoft Unified Communications software.

In MX-ONE 5.0 SP1, TR-87 support for CSTA III (Computer Supported Telecommunications Applications Version 3) was added to allow a third party application to control an MX-ONE device via CSTA and SIP messages. This service can be used, for example, to connect MX-ONE and Microsoft Lync Server via a function called Remote Call Control.

Mitel has performed an internal integration validation between MX-ONE 6.0 and Lync Server 2013 via Remote Call Control, where several tests were executed to assure the compatibility between the products.

Scope

The intent of this guide is to describe the setup tasks to integrate MiVoice MX-ONE and Microsoft Lync Server 2013 for Remote Call Control.

For more details regarding components of this integration, we refer to the relevant MX-ONE CPI documentation or, please, go to the Microsoft Lync Server 2013 product website.

	Note! Always check the latest products documentation.

Solution Description

Integration of MX-ONE 6.0 with Microsoft Lync Server 2013 for Remote Call Control as a complementary solution, provides users enabled for remote call control to use Lync 2013 client to control calls on their MX-ONE phones.

MiVoice MX-ONE

MiVoice MX-ONE has a built-in CSTA III server that is an interface that other applications can use to remotely control a phone. Examples of operations that can be performed with CSTA Phase III are: make call, answer call, dial a number and terminate a call.

MX-ONE 6.0 supports CSTA method that is based on European Computer Manufacturers Association (ECMA) Technical Report-87 (TR-87), called Using CSTA for SIP Phone User Agents (uaCSTA). MX-ONE implements a subset of the capabilities and methods proposed in TR-87 specification.

In TR-87 (Using CSTA for SIP Phone User Agents (uaCSTA)):

SIP is used to establish a CSTA application session

CSTA service request and response messages are transported over SIP

CSTA monitor is started and CSTA events are transported over SIP

Microsoft Lync Server 2013

Microsoft Lync Server 2013 offers Remote Call Control (RCC) support that allows users to remotely control phones connected to a call manager, such as MX-ONE. It gives Lync 2013 client users the ability to make or receive calls on their fixed or mobile phone instead of a computer.

Integration

CSTA III (XML) is required to provide the integration between MX-ONE and Lync Server for Remote Call Control as shown in the figure below.

The telephony feature commands are sent from the Lync 2013 client through the Microsoft Lync Server 2013 to the internal MX-ONE CSTA server as CSTA III messages over SIP, so called user agent CSTA (uaCSTA). The internal MX-ONE CSTA server analyzes the requests and maps them to the corresponding CSTA commands towards MX-ONE, which will then carry out the requests.

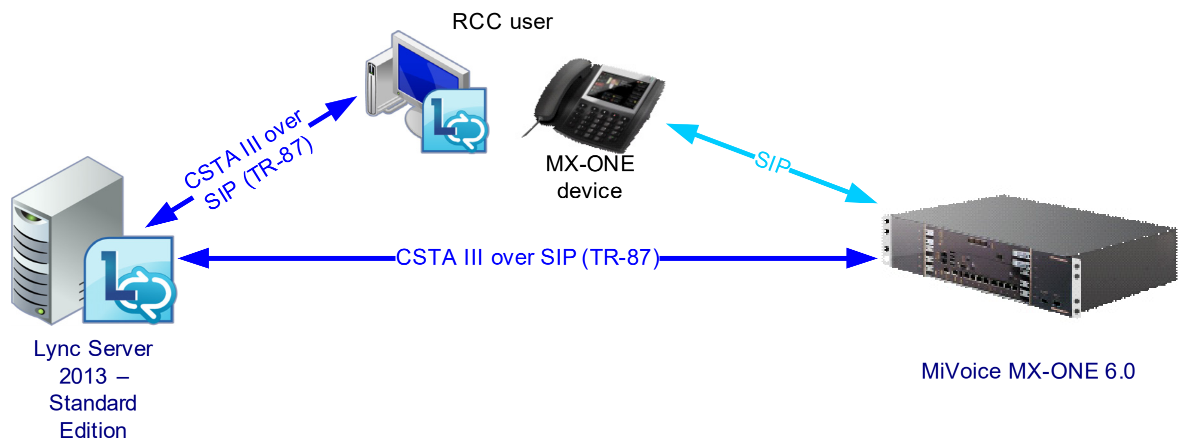


Figure 1 - Integration via Remote Call Control (RCC) between MX-ONE and Lync Server 2013

With Microsoft Lync Server 2013 integration, it is possible from Lync 2013 client (Remote Call Control Only) to manage calls and talk using any fixed and remote extensions within the MX-ONE.

The features that a Lync 2013 client can manage when integrate with MX-ONE using RCC are:

Make an outgoing call

Answer an incoming call

Transfer a call to another user (monitored transfer with current conversations)

Single step transfer

Forward an incoming call to an internal number (internal and private network extensions)

Forward an incoming call to an external number

Redirect an incoming call

Place calls on hold

Alternate (toggle) between multiple concurrent calls

Answer a second call while already in a call.

Dial dual-tone multi-frequency (DTMF) digits

Requirements and Setup

MX-ONE and Microsoft Lync needs to be configured in different sip domains. Mitel recommendation is that MX-ONE is a sub-domain of the Lync domain.

For example, Lync runs on the domain: domain.com and MX-ONE runs on the domain: mx-one.domain.com.

MIVOICE MX-ONE Requirements

Software and licenses required for Microsoft Remote Call Control integration:

MiVoice MX-ONE Service Node 6.0 or later

MX-ONE licenses for:

CSTA III

	Note! Multi terminal extensions cannot be monitored via CSTA and therefore it does not work in the Remote Call Control scenario.

Microsoft Lync Server 2013 Requirements

The Microsoft infrastructure (AD, DNS, CA, etc) needs to be in place, including all licenses required.

This guide does not cover the Lync Server 2013 installation. Our recommendation is that the Microsoft infrastructure shall be installed by a trained Microsoft engineer.

Before to start Microsoft Lync Server 2013 for RCC setup, read the following document:

Microsoft Lync Server 2013, Deploying Remote Call Control

http://technet.microsoft.com/en-us/library/gg558664.aspx

	Note! This Microsoft documentation is used in conjunction with this guide.

MX-ONE was validated with Microsoft Lync 2013 Remote Call Control with only one Lync Front End server.

Microsoft Lync 2013 requires load balancer when more than one Front End is used. Please note that this setup was not validated with MX-ONE.

	Note! The latest Lync Client (Lync 2013 update: April 2014) needs to be installed in the end user computers, please see that article below.

http://support.microsoft.com/kb/2880474

Integration Setup - TCP

The setup used in this guide is based on the following scenario:

One Microsoft Lync Server - Standard Edition connected with one MiVoice MX-ONE 6.0.

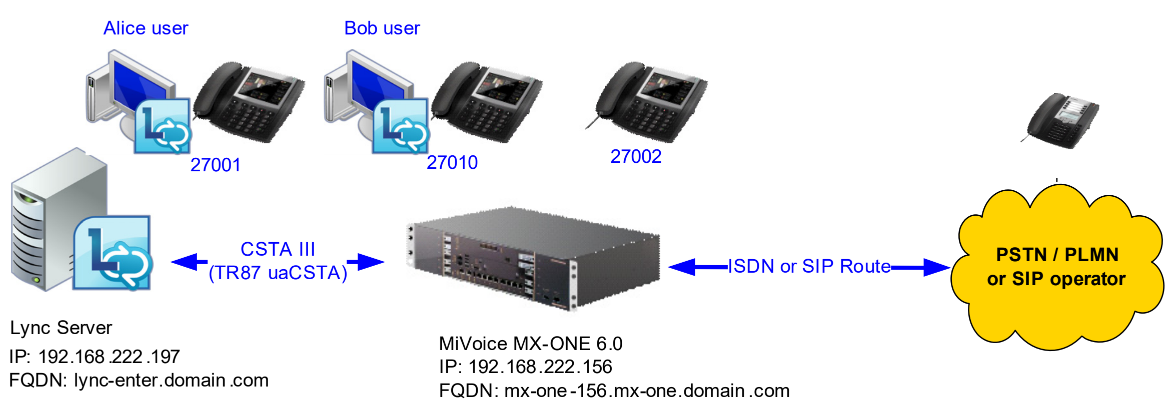


Figure 2 - Integration setup

	Note! Mitel recommends that complex scenarios shall be validated in the partner labs prior to customer deployment.

MiVoice MX-ONE Setup - TCP

The following shall be configured:

CSTA server needs to be initiated

Creating CSTA Server

CSTA III Setting:
csta--initiate--lim1 --csta-serv00000010

For more about CSTA III, see MX-ONE CPI documentation.

Microsoft Lync Server 2013 Setup – TCP

The following setup is based in the Microsoft Lync Server 2013 documentation, Deploying Remote Call Control, for more about commands syntaxes check:

http://technet.microsoft.com/en-us/library/gg558664.aspx

The following shall be configured:

Configure a Static Route for Remote Call Control

Configure a Trusted Application Entry for Remote Call Control

Configure Static Route for Remote Call Control

The following commands shall be executed in the Lync Server Management Shell to configure Remote Call Control.

Route for Remote Call ControlSetup, port 5060 (TCP):
$TCPRoute= New-CsStaticRoute-TCPRoute-Destination 192.168.222.156 -Port 5062 -MatchUrimx-one.domain.com
Set-CsStaticRoutingConfiguration-Route @{Add=$TCPRoute} -Identity Global
To verify the setup use the command:
Get-CsStaticRoutingConfiguration

Configure a Trusted Application Pool Entry for Remote Call Control

To create a Trusted Application Pool use the command:
New-CsTrustedApplicationpool-Identity 192.168.222.156 -Registrar lync-enter.domain.com –Site 1 –TreatAsAuthenticated$True –ThrottleAsServer$True
To verify the setup use the command:
Get-CsTrustedApplicationpool

Configure a Trusted Application Entry for Remote Call Control

To setup the trusted application use the command::
New-CsTrustedApplication-ApplicationIDRCC -TrustedApplicationPoolFqdn192.168.222.156 -Port 5062 -EnableTcp
To verify the setup use the command:
Get-CsTrustedApplication

Publish the topology

To implement the changes in the Lync , publish the topology
Enable-CsTopology

Define a SIP/CSTA Gateway IP Address

In this example TCP is used, then the SIP/CSTA gateway IP address needs to be defined. Follow the instruction in the session “Define a SIP/CSTA Gateway IP Address” from Microsoft documentation: http://technet.microsoft.com/en-us/library/gg602125.aspx.

When the setup is done, the Topology Builder screen should be similar to figure below.

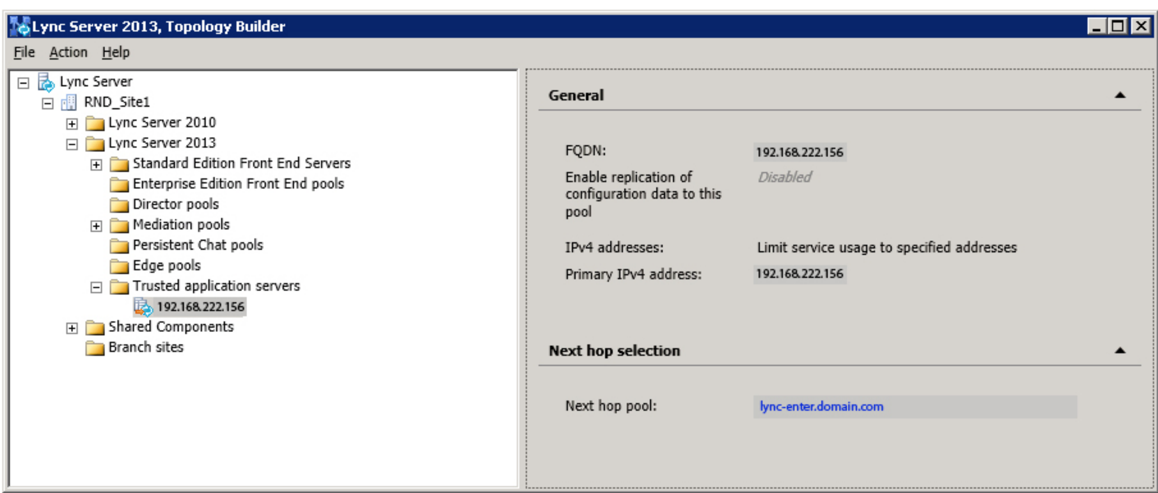


Figure 3 - Lync Server 2013 Topology Builder

Enable Lync Users for Remote Call Control

Configure a user for remote call control by using Lync Server Control Panel.

Under Telephony, select Remote Call Control Only. Please, note that the option “Remote Call Control” is not supported by MX-ONE.

The following needs to be configured under Line URI and Line Server URI.

Enable Lync Users for Remote Call Control:
Line URI:tel:phonenumber, exampletel:27000

Line Server URI:sip:tel@MatchUri, for example: sip:27000@mx-one.domain.com

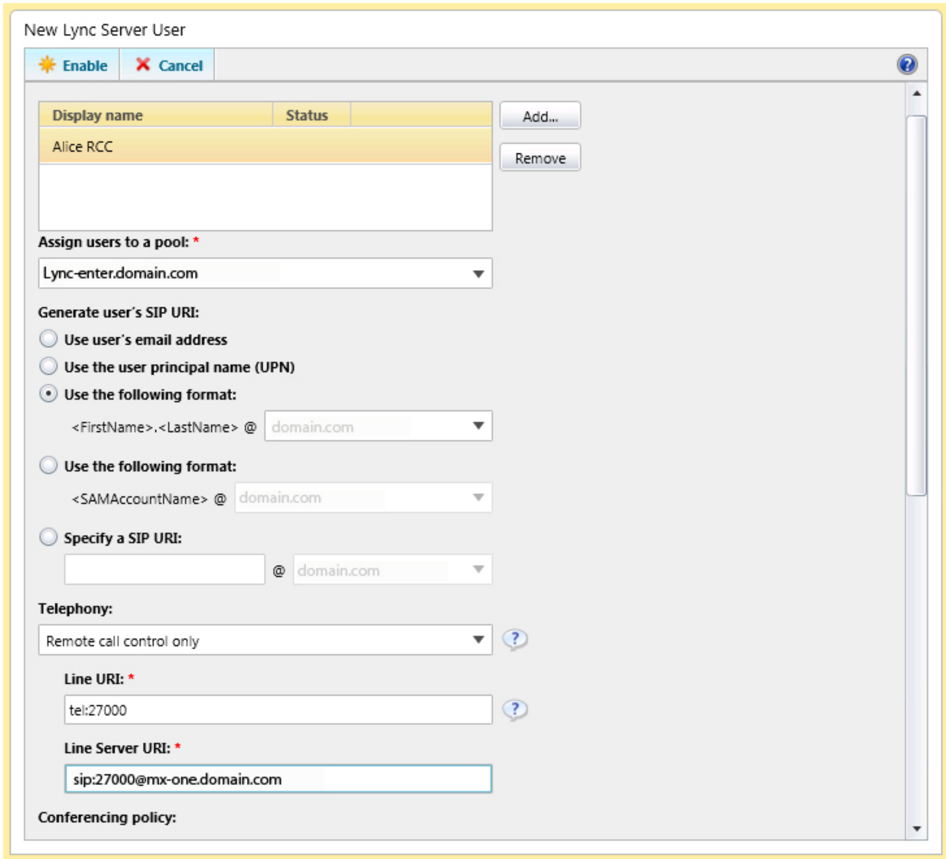


Figure 4 - RCC only new user configuration example

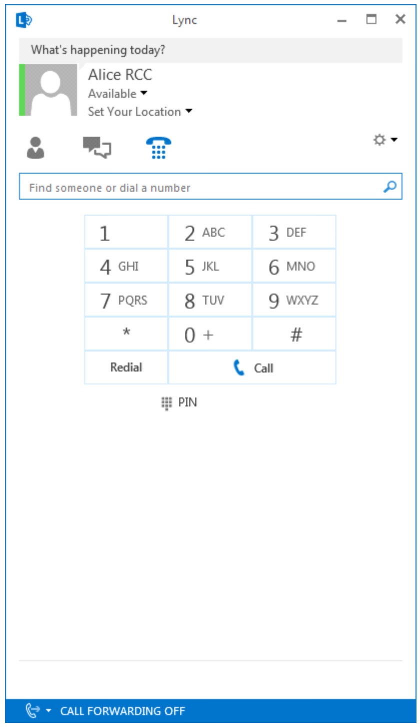
How to Verify the Setup

After completing the setup, the integration can be verified in the following way:

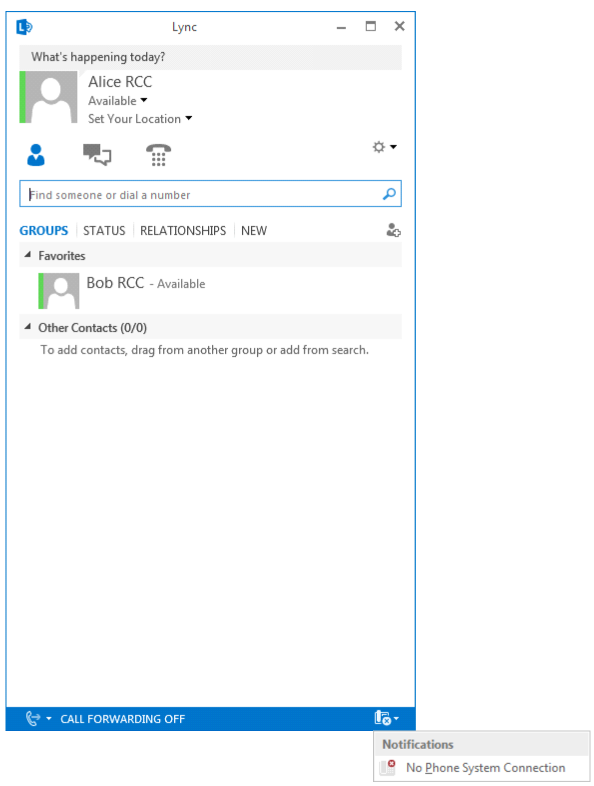
Lync 2013 Client Features

Using a Lync 2013 client sign-in a RCC user.

If the configuration was done properly the user will be signed in without any error, see the figure below.



If there is small icon in the lower right side of the Lync 2013 client, showing a phone with an error, check the setup, because the CSTA monitoring could not be established.



Use the MiVoice MX-ONE command “csta -p --lim all --devices” to check the devices that are monitored.

In the use cases below two Lync clients were used and three MX-ONE extensions.

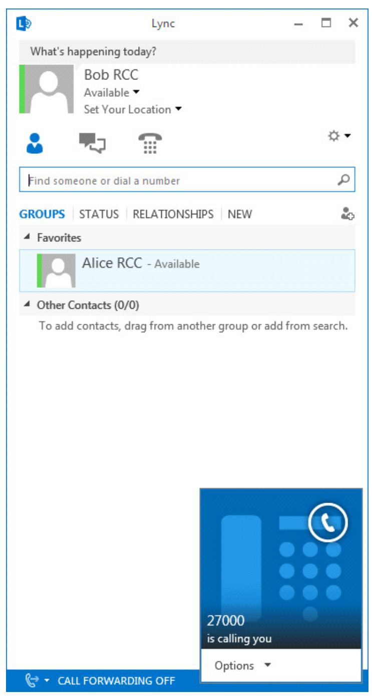
1. Alice.RCC controls the extension 27001, which is a SIP extension in MX-ONE.
2. Bob.RCC controls the extension 27010, which is a SIP extension in MX-ONE.
3. 27000 and 27002 are SIP extensions in MX-ONE.
4. 33350202 and 33350102 are the PSTN phones.

Make an Outgoing Call Using the Lync 2013 Client

From extension A use the Lync client (RCC) to dial extension B, pick up your handset as soon as you hear the ring back tone, wait the extension B answer, check if there is speech.

Answer an Incoming Call

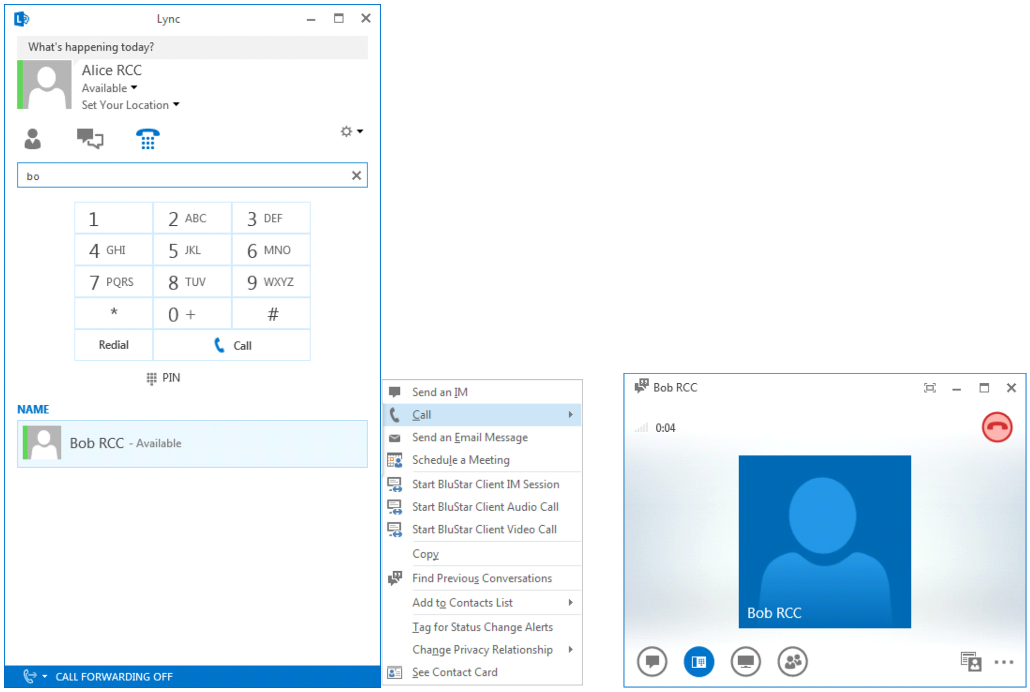
From another extension dial to RCC user, answer it and check if there is speech.



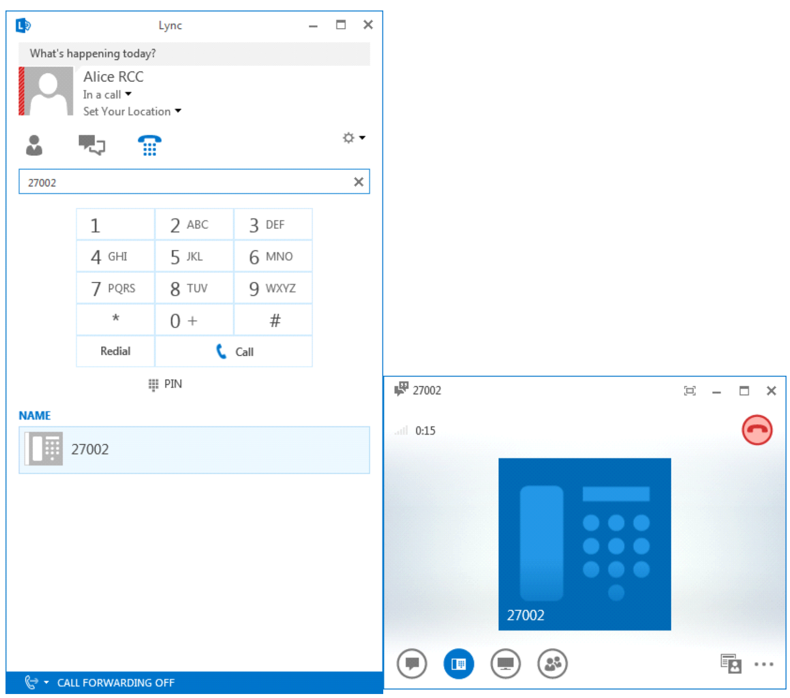
Transfer a Call Between Current Conversations (Monitored Transfer)

In this scenario A (Alice.RCC - extension 27001) calls B (Bob.RCC - extension 27010), A puts B on hold and then calls extension C (27002). After C answers, A transfers the call between B and C.

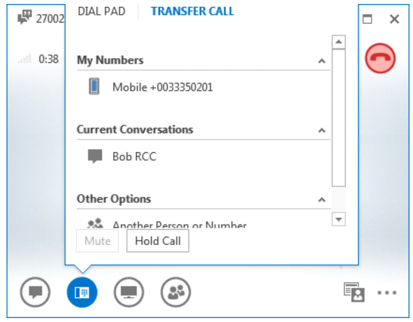
We assume you have answered a call with extension B (27010) from the Lync client (RCC



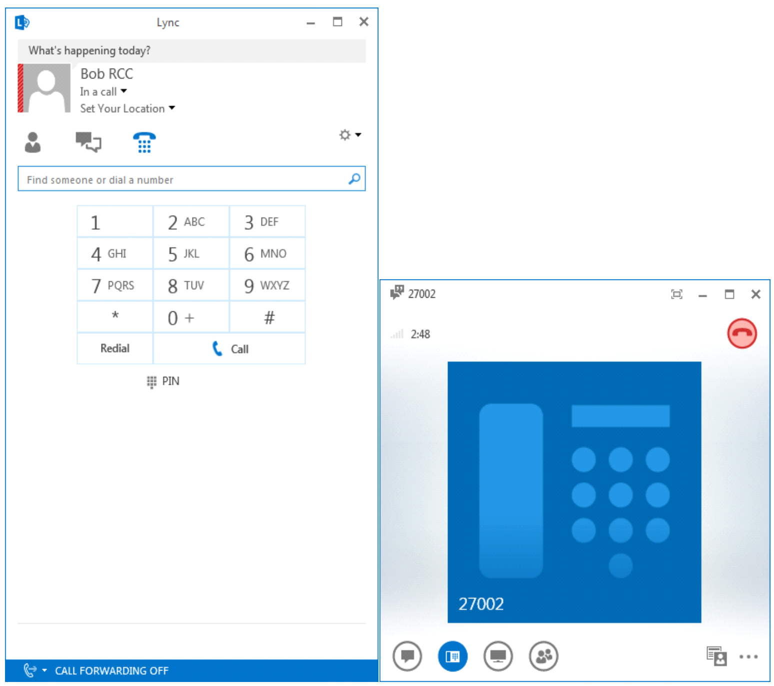
Using the client, put extension B on hold and make a second call to extension C (27002), and wait until the extension C answers.



Once speech is established, initiate the transfer of extension B (Bob RCC) using the Current Conversations option as shown below.



Then, check if the call is correctly transferred.

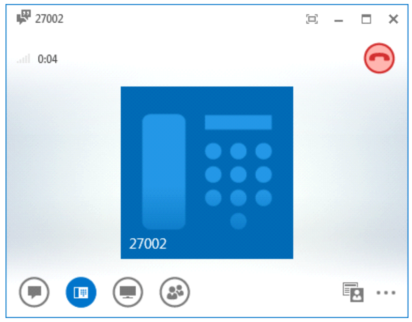


Then, check if the call is correctly transferred.

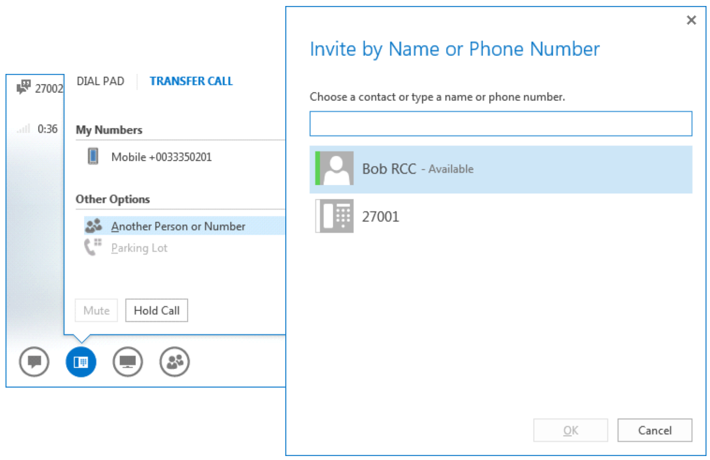
Single Step Transfer

In this scenario A (Alice.RCC - extension 27001) is talking with C (extension 27002), A transfer C directly to extension B (Bob.RCC - extension 27010).

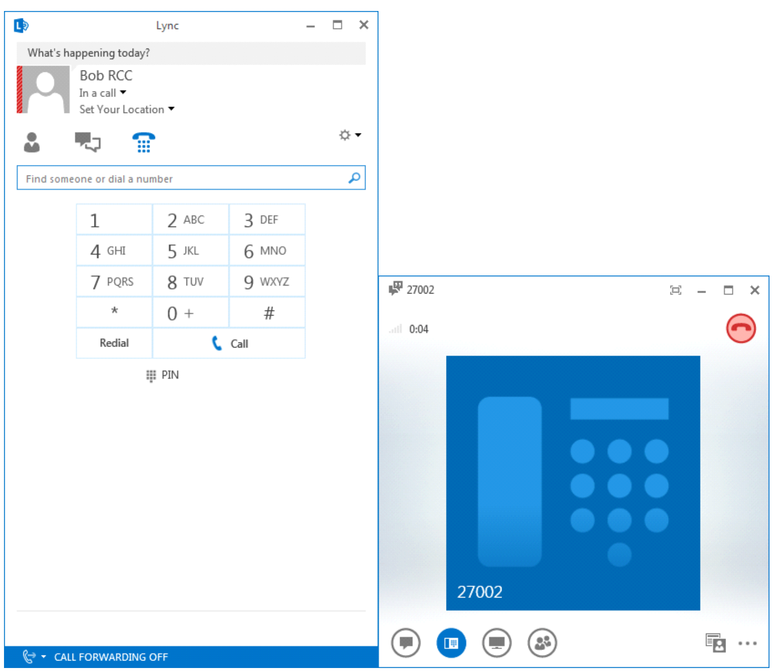
We assume you have answered a call with extension C (27002).



A does single-step transfer from extension C (27002) to B (Bob.RCC - extension 27010).

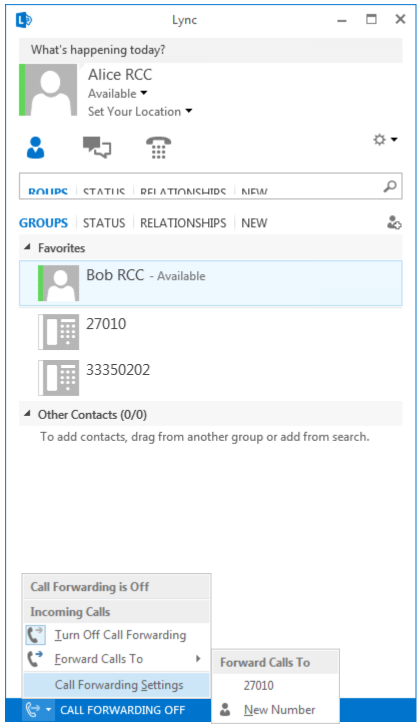


Then, check if the call is correctly transferred.

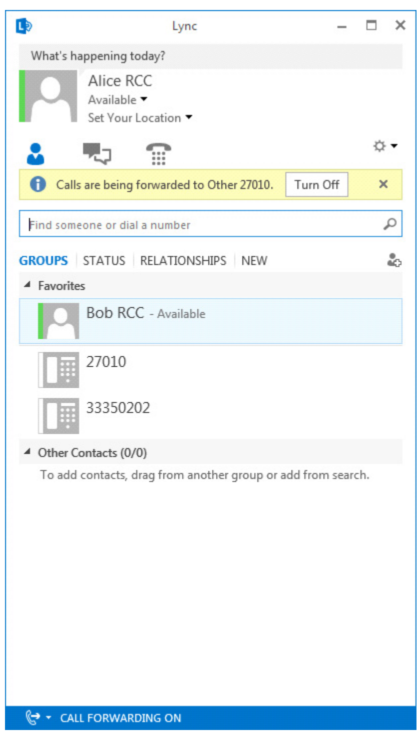


Forward an Incoming Call

Select a predefined or a new number (internal, network extension or external) and click ok.

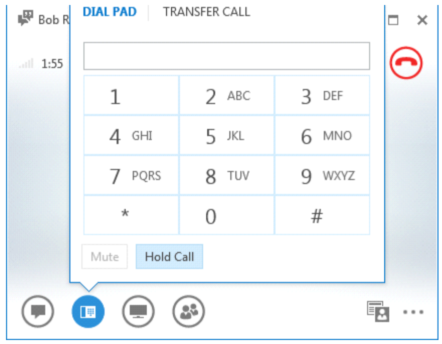


Check if Lync client is showing that the forwarding is on.

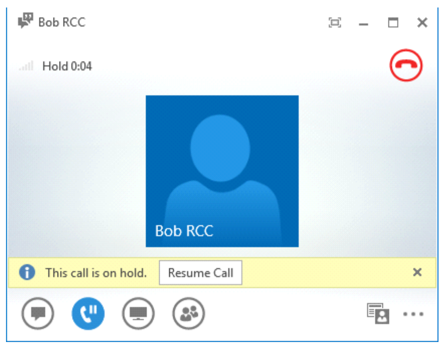


Place Calls on Hold

When in speech, press the hold button to hold a call.

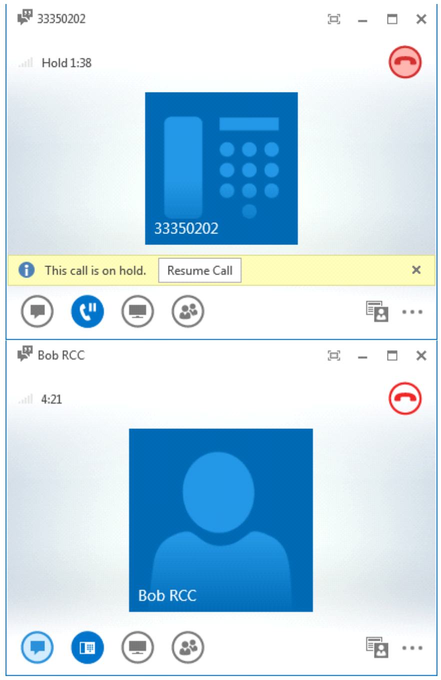


Click on Resume Call to return to the call.

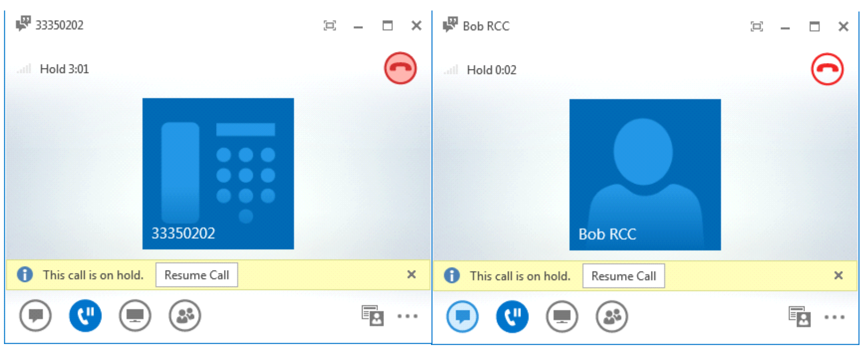


Alternate Between Multiple Concurrent Calls

When connected with two calls, press the hold button to hold a call and click on Resume Call to return to

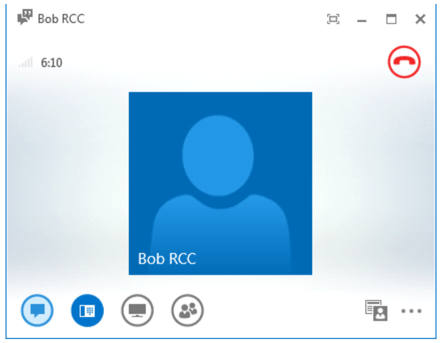


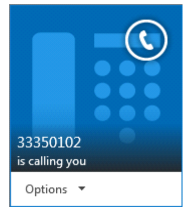
the first one.



Answer a Second Call While Already in a Call (call waiting)

When a second call is alerting, click on Accept Call to answer it.

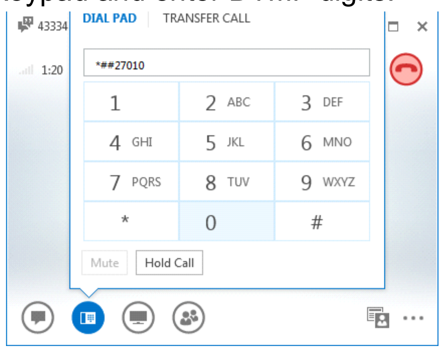




You can alternate between the calls.

Dial Dual-Tone Multi-Frequency (DTMF) Digits

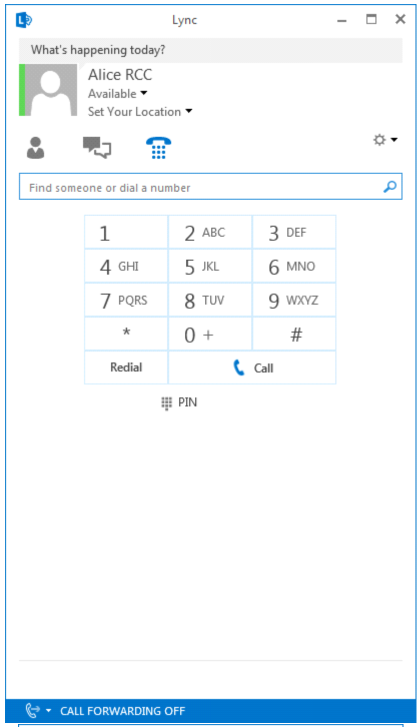
In an established call, click on the keypad and enter DTMF digits.

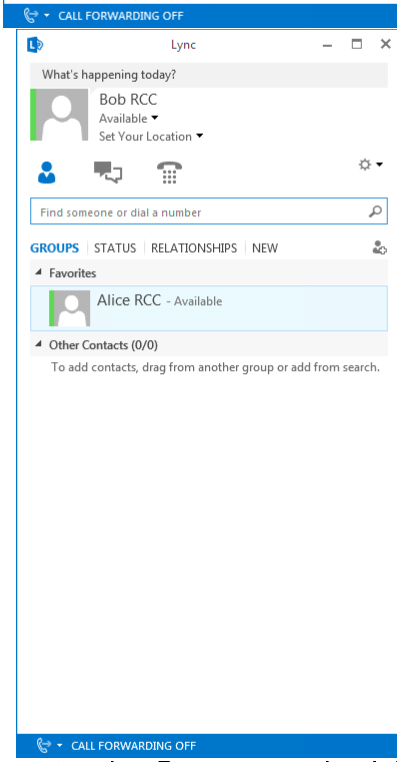


Presence

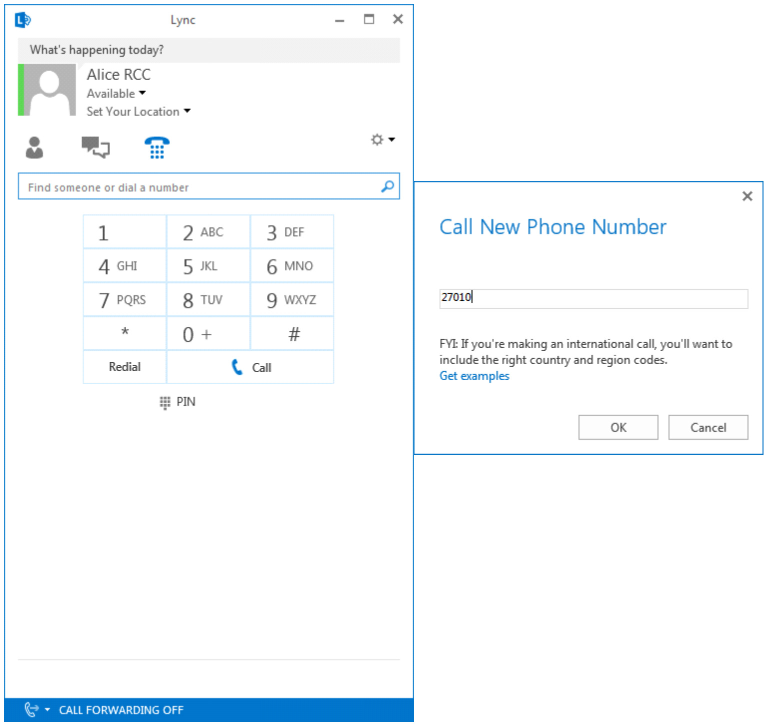
In order to verify presence, establish a call using Lync client (RCC) as below.

From extension A use the Lync client (RCC) to dial extension B, pick up your handset as soon as you

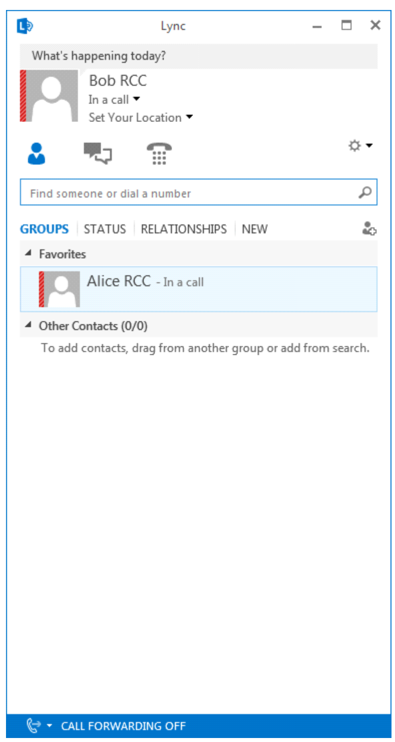




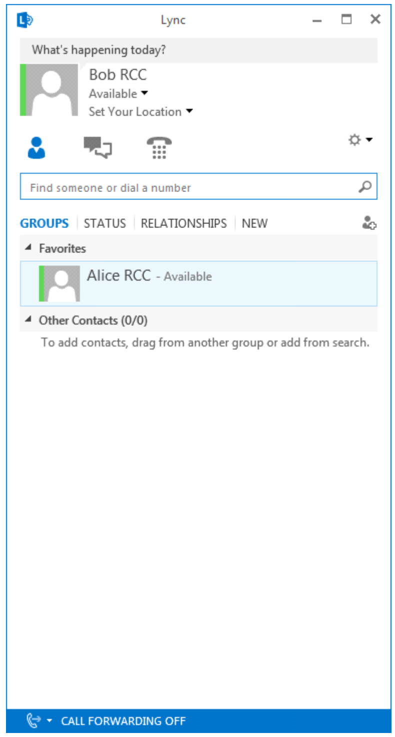
hear the ring back tone, wait until the extension B answers, check if there is speech.



From another Lync client, for example Bob, RCC that is monitoring Alice RCC, check if the presence status is now “In a Call”.



Disconnect the call from extension A (Alice RCC) and check if the Alice RCC presence status goes to Available in the Bob RCC.



Limitations

The integration supports Lync 2013 clients configured with “Remote Call Control only” option. The option “Remote Call Control” is not supported.

The secure transport mechanism using TLS is not supported in MX-ONE 6.x.

The features listed below are not supported in this integration, when initiated by the Lync client:

Do not disturb (it is not supported by Lync client)

	Note! Although these features may not be possible from the client, they may be invoked directly on the terminal instead.

Good to Know

MX-ONE and Lync Server cannot be part of the same domain.

Latest Lync client needs to be installed.

DNS needs to be properly configured.

Conference can be invoked via Lync client using MX-ONE procedure (normally dialing 3). However, the Lync client will merge all other screens with the first one and that will be presented until the last member disconnects.

Revision History

Document Version	Comment	Date
Rev. A	First release	2014-05-09
Rev. B	Rebranding	2015-05-10
Rev. B1	Some further rebranding corrections done.	2016-03-17
Rev. B2	Minor changes done.	2016-10-10

Teleworker Solution

Customer Product Information of MiVoice Border Gateway, see Product Documentation.

General

This document describes how to configure a single standalone MiVoice Border Gateway (MBG) Release 9.2 server to support Mitel 6900/6800 SIP Terminals as Tele-worker devices for MX-ONE.

This document complements MX-ONE document “Mitel 6700i and 6800i SIP Terminals for MX-ONE” and provides instructions how to setup MBG as an Ingate replacement. The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and unsecured communication on the inside towards MX-ONE. The proposed solution has the same limitations as the existing Ingate deployment.

Instructions in this document are specific to the above configuration and must NOT be used in any other deployments. For example, MiCollab 7.1 with MBG and MiCollab clients with MX-ONE.

Application Requirements

You must meet the minimum software level requirements for each application listed below so that the applications function correctly with this Release.

Application	Recommended Software Level	Comments
Mitel Standard Linux (MSL)	10.4.13.0	Release 10.4 64 bits is required. Refer to the Hardware Compatibility List for MSL found on Mitel-On-Line.
MX-ONE	6.3	MX-ONE version 6.0 SP2 HF3 was tested in the Kanata lab, so this version, or later, could be used, but 6.3 is recommended.
6900	5.0.0	Release 5.0 SIP extensions
68xxi	4.2.0.181	Release 4.2 Release 4.2 SP1 recommended.
MBG	4.2.0.181	Release 9.2 PR2 and up recommended.

Installation Notes

The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and unsecure communication on the inside towards MX-ONE.

Licensing

The only licensing required is a MiVoice Border Gateway base kit (physical or virtual) and Teleworker licenses (1 per 68xxi device + a few floater licenses).

Installing Release 9.2 on a standalone physical server

1. Install the latest Microsoft SQL (MSL) 10.4 64 bits release software version.
2. Install Release 9.2 via MSL's server-manager Blades panel after syncing with the Mitel Application Management Center (AMC); or,
3. Obtain a copy of the latest MiVoice Border Gateway Rel 9.2 software and burn it onto a CD. After inserting the CD in the CD-ROM/DVD-ROM drive, upgrade via MSL's server-manager Blades panel.

Note: Your CD burning software must be capable of burning ISO images.

Installing Release 9.2 in a VMware environment

Virtual deployment should deploy the latest released MBG 9.2 ova and then upgrade to the latest available blade of that stream.

Firewall Configuration

If MBG is deployed in a demilitarized zone, the following ports need to be opened (above ports needed for communication with the AMC).

- TCP port 5061 between the Internet and MBG for SIP TLS
- TCP port 5060 between MBG and MX-ONE
- TCP port 22223 between the Internet and MBG for SIP XML
- TCP port 22222 between MBG and MX-ONE for SIP XML
- TCP port 4431 between the Internet and MBG for Configuration Server Access (Optional)
- TCP port 80 between MBG and the Configuration Server

- UDP port 20000-31000 between the Internet and MBG and between MBG and the LAN for voice
- TCP port 22 between LAN and MBG for secure shell access
- UDP port 53 between MBG and the LAN for DNS resolution to a Corporate DNS server

Note: Do not enable TCP port 5060 or UDP port 5060 between the Internet and MBG.

MSL Configuration

1. Configure your MSL server to use a Corporate DNS server that can resolve any FQDN associated with MX-ONE.

2. Configure your MSL server to allow Remote Access for secure shell from a local network. This access will be needed to run a special setup script.

3. Navigate to Remote Access under MSL Server Manager.

4. Select “Allow access only from trusted and remote management networks” to setup secure shell access.

5. Select “Yes” for administrative command line access over secure shell.

6. Select “Yes” to allow secure shell access using standard passwords.

MBG Configuration

From a new installation of Release 9.2, access the MiVoice Border Gateway User Inter-face from MSL server-manager and perform the following steps:

1. Go to System Configuration > Network Profile.

a Select Profile and Apply.

2. Go to System Configuration > Settings.

a Under SIP options, increase the Set-side registration expiry time to 360 from the default of 240.

b Enable SIP support for TCP/TLS and TCP.

c Change Codec support to Unrestricted.

d Change Set-side RTP security to Require (to enforce SRTP between the phone and MBG).

Note: Optionally, you can disable support for all protocols under Minet Support.

3. Service Configuration > ICPs

a Add your MX-ONE system as type MiVoice MX-ONE with SIP capabilities as UDP, TCP.

b Configure MX-ONE support.

c Check Link to the ICP and Enable.

d Configure the XML listen port as 22223 and check TLS.

e Configure the XML destination port as 22222 and uncheck TLS.

f Configure the configuration server listen port as 4431 and check TLS.

g Configure the configuration server port as 80 and uncheck TLS.

h Configure the configuration server address.

Note: Only provide access to the configuration server if ALL the files in all the directo-ries are encrypted with anacrypt. If not, enter a bogus IP address to not expose the internal configuration server to the Internet. The InGate solution has the same exposure.

i Click Save.

4. Do not start MBG yet.

5. Setup MBG with mutual TLS for SIP using configuration script.

6. Connect to the system via ssh (ex: using putty) and login as root.

7. Run the configuration script specifying the MBG Public IP address (i.e the address the Teleworker 68xx phones will connect to) and the MBG local or LAN IP address.

Optionally, you can use the script to modify an existing mitel.cfg or use MBG as a TFTP server for the phones.

To view all options available, run the configuration script without arguments.

[root@mysystem ~]# /usr/sbin/configure_68xx_mbg_support.sh

Example #1: MBG Public IP is 1.1.1.1 and MBG local IP is 192.168.100.10

[root@mysystem ~]# /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip ip_ad-dress --mbg_lan_ip ip_address --generate_certificate

[root@mysystem ~]# /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip 1.1.1.1 --mbg_lan_ip 192.168.100.10 --generate_certificate

mbg_wan_ip=1.1.1.1

mbg_lan_ip=192.168.100.10

configure_tftp=false

generate_certificate=true

force=false

creating /root/aastra_tftp, output files will be placed there.

configuring mbg certificate with ip address: 1.1.1.1

Generating a 2048 bit RSA private key

....+++

....+++

writing new private key to '/root/aastra_tftp/mbg_mxone_key.pem'

-----

writing RSA key

details:

InsertCertificateIntoChain

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

ReorderCertificateChain:: client certificate found:

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

ReorderCertificateChain:: root CA certificate found:

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

VerifyCertificateChain:: m_vrCerts.size()=1 rc=1

certificate and key files for set are /root/aastra_tftp/mbg_mxone_cert.pem and /root/aastra_tftp/mbg_mxone_key.pem

done.

Example #2: MBG Public IP is 1.1.1.1, MBG local IP is 192.168.100.10, modify an existing mitel.cfg (transferred to /root

[root@mysystem ~]# /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip 1.1.1.1 --mbg_lan_ip 192.168.100.10 --generate_certificate --modify_cfg_template mitel.cfg --ntp_server pool.ntp.org --time_zone_name SE-Stockholm

mbg_wan_ip=1.1.1.1

mbg_lan_ip=192.168.100.10

configure_tftp=true

generate_certificate=true

force=false

will configure tftp directory /root/aastra_tftp to serve up config files

creating /root/aastra_tftp, output files will be placed there.

configuring mbg certificate with ip address: 1.1.1.1

Generating a 2048 bit RSA private key

....+++

..........+++

writing new private key to '/root/aastra_tftp/mbg_mxone_key.pem'

-----

writing RSA key

details:

InsertCertificateIntoChain

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

ReorderCertificateChain:: client certificate found:

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

ReorderCertificateChain:: root CA certificate found:

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

VerifyCertificateChain:: m_vrCerts.size()=1 rc=1

certificate and key files for set are /root/aastra_tftp/mbg_mxone_cert.pem and /root/mitel_tftp/mbg_mxone_key.pem

creating mitel.cfg from template, configured with MBG's CN ip

sip proxy ip

sip proxy port

sip registrar ip

sip registrar port

sip outbound proxy

sip outbound proxy port

tftp server

sips trusted certificates

sips root and intermediate certificates

sips local certificate

sips private key

https validate certificates

https user certificates

time server disabled

time server

time zone name

sip transport protocol

found URL's pointing to 22222, switching to https and port 22223

appending fixed URLs to config file

done.

8. Return to the MiVoice Border Gateway User Interface and click on Dashboard to

Start MBG

9. Confirm that Teleworker 68xx phones have access to the public IP of MBG using the Teleworker Network Analyzer tool.

10. Download the tool from Administration – File Transfer and install it on a Windows machine that has network connectivity to the public IP of your system.

11. Launch the application and run a connect test against the public IP.

SIP TLS, Aastra MXL MXOne, Voice Traffic (begin) and (end) should return OK.

If any of the above return CLOSED or TIMED OUT, contact your firewall administrator.

Phone Configuration

1) Phone must be staged in the office.

2) Using WinSCP, copy the /root/aastra_tftp/mbg_mxone_cert.pem and /root/aastra_tftp/mbg_mxone_key.pem to a special folder (ex: athome) on your configuration server.

3) Append the settings listed in “Appendix – mitel.cfg Settings” to your mitel.cfg file or used the modified mitel.cfg also available under /root/aastra_tftp.

If needed, update all other files (ex: <model.cfg>) to use https/22223 instead of http/22222.

Limitations

A list of known limitations shared with the InGate solution.

1) Phones must be staged in the office.

2) Phone firmware must be done in the office as a phone firmware upgrade will remove the certificate loaded.

3) Access to internal configuration server cannot be limited/controlled/blocked from the outside.

4) 68xxi must have access to a NTP server for certificate validation.

5) Corporate directory access must be setup with port forwarding on MSL (server-gateway configuration) or the DMZ firewall.

6) If MX-ONE is setup to like lim1.mysystem.com, the MSL server must point to a Corporate DNS to allow proper DNS resolution.

Here is a list of known limitations with MBG

a) Single dedicated MBG.

b) MBG clustering and backup SIP registrar/proxy in the 68xxi configuration files.

c) Using FQDN instead of IP address in the 68xxi configuration files.

Known Issues

None.

Issues Resolved

Here is a list of issues resolved in 9.2.0.22 in conjunction with 68xx 4.2 SP1 firmware and workaround is not longer required:

1) MN00609195 MBG 9.2: SIP 68xxi/MX-One/SRTP one way audio after “set side” session timer re-invite (decrypt failure).

2) Conditions: Session timers are configured on TW 68xxi AND greater than 1310 (default in MX-ONE sample is 1800).

3) Root Cause: 68xxi do NOT increment SDP version but changes SRTP keys in re-invite and MBG falsely detects the SDP as a duplicate.

4) Workaround: Select a value less than 1200 for session timers in mitel.cfg for TW 68xxi.

5) MN00616730 MBG 9.2: SIP 68xxi/MX-One/SRTP one way audio after "ICP side" session timer re-invite.

6) Conditions: Session timers are configured on LAN 68xxi AND greater than 1300 AND the codec list is different between LAN and TW set but 1st selection is the same.

7) Root Cause: Still under investigation.

8) Workaround #1: Same codec selection list on TW 68xxi as LAN 68xxi (MX-ONE sample has G.722, G711a, G.711u, G.729. Updates are used instead of re-invite.

9) Workaround #2: Disable session timers in mitel.cfg for LAN 68xxi or reduce the value to 1200 or less.

Upgrade Notes

Trials sites that have deployed based on earlier versions of this document, need to run the following command on their system to ensure that all required files are part of a backup.

[root@mysystem ~]# db tug setprop config backuplist /etc/tug/tug.ini.certifi-cates.ini,/etc/tug/tugcerts.ini,/etc/tug/ca-bundle.crt,/etc/tug/mbg_mxone.ini

Appendix - Config Script

[root@ ~]# /usr/sbin/configure_68xx_mbg_support.sh

mbg_wan_ip=

mbg_lan_ip=

configure_tftp=false

generate_certificate=false

force=false

--mbg_lan_ip parameter must be specified

Usage: /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip ip_address --mbg_lan_ip ip_address [--tftp] [--generate_certificate] [--force] [--modify_cfg_tem-plate aastra_cfg_file_template] [--ntp_server fqdn/ip] [--time_zone_name aastra_name_string]

--mbg_wan_ip - MBG public address

sets connect to this address and MBG certificate will contain this

--mbg_lan_ip - MBG private address

used for SIP udp and tcp communications with ICP
(udp and tcp are disabled on MBG's public address)
--tftp - configure this MBG to supply configuration files via tftp
--generate_certificate - create a certificate using the value supplied for 'mbg_wan_ip'
--force - override 'certificate already exists' check
--modify_cfg_template - If set, specified file will be modified.
Cfg settings dealing with certs/sip will be adjusted
--ntp_server - If set, specified fqdn will be used for ntp settings.
otherwise 'pool.ntp.org' will be used.
--time_zone_name - If set, specified time zone string will be used for ntp settings.
otherwise 'SE-Stockholm' will be used.

Appendix - mitel.cfg Settings

```
#-----------------------------------------------------------------
# MiVoice Border Gateway (MBG) Teleworker features
# SIP TLS and SRTP between the phone and MBG
# HTTPS used for XML
#-----------------------------------------------------------------

# MBG is the SIP proxy and registrar
sip proxy ip:MBGIP
sip proxy port:5061
sip registrar ip:MBGIP
sip registrar port:5061
sip outbound proxy:MBGIP
sip outbound proxy port:5061  #5061 or 0(which will attempt SRV and as fall back send to 5061 due to TLS)

# Persistent SIP TLS (requires 'sip outbound proxy')
sips persistent tls:1
sip outbound support:1
sip transport protocol:4 #4-TLS

# Certificates/keys for sip-tls
sips trusted certificates: mbg_mxone_cert.pem
sips root and intermediate certificates: mbg_mxone_cert.pem
```

sips local certificate: mbg_mxone_cert.pem

sips private key: mbg_mxone_key.pem

https validate certificates: 1

https user certificates: mbg_mxone_cert.pem

Voice Encryption (SRTP)

sip srtp mode:2

OPTIONAL – Use MBG's TFTP server

#tftp server:MBGIP

#NTP server must be accessible from the home network

time server disabled: 0

Time server1:<NTP server>

Action URI must use HTTPS to port 22223

action uri startup:https://$$PROXYURL$$:22223/Startup?user=$$SIPUSERNAME$$

services script: https://$$PROXYURL$$:22223/Services?user=$$SIPUSER-NAME$$&voicemailnr=

#--

Note: Similar changes may be required to <model>.cfg or <mac>.cfg files.

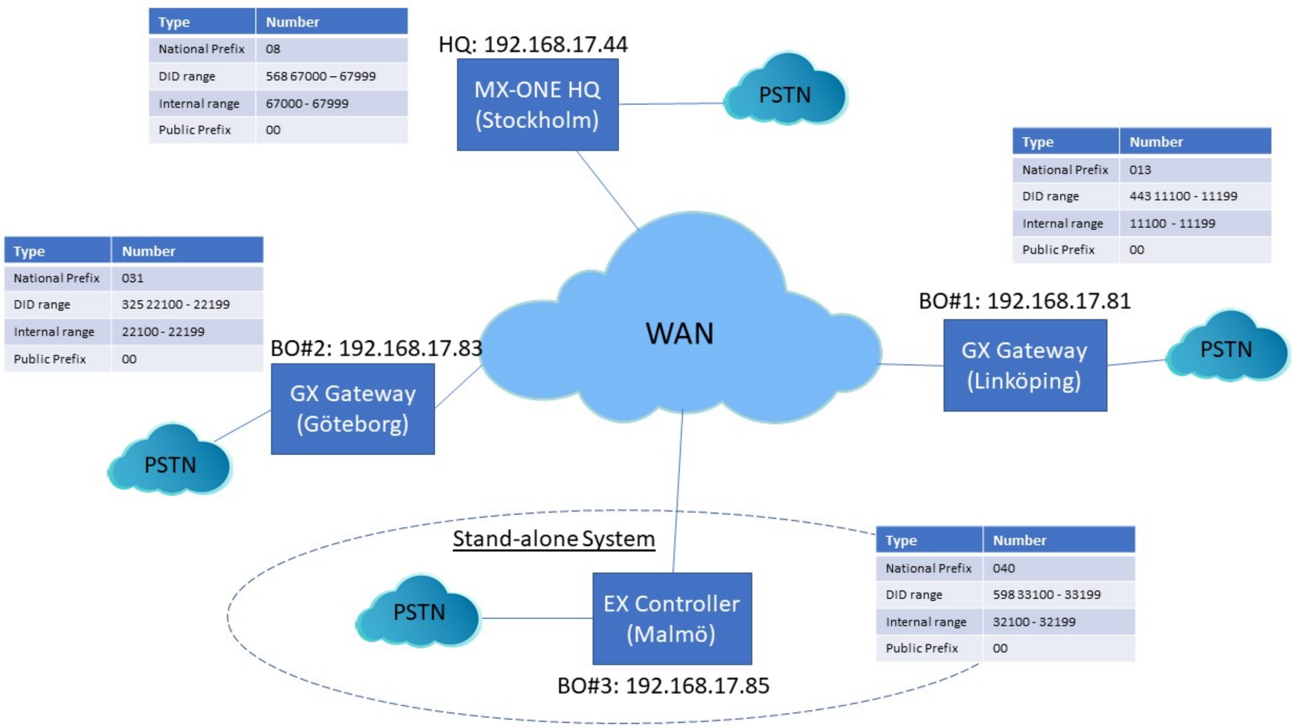
GX and EX Controller

The GX and EX controller installations are explained in this topic.

Introduction

This document describes a typical scenario for a branch office with survivability and local presence. It contains both the GX and the EX gateways.

Figure 11.1: EX and GX Controller Gateways



NOTE: The EX gateway can only be used as a stand-alone system.

Prerequisites

When planning the number series in the branch office following must be considered:

- The extension range must be coherent and matching the local DID number series (if local presence is used).
- MX-ONE SW must be at least version 7.0.
- The firmware level of the EX-Controller and GX-Gateway shall be at least **Dgw 42.3.1032-MT** with profile **S100-MT-D2000-45** for GX-Gateway and **STNL-MT-D2000-65** for EX-Controller.

Other considerations/restrictions:

- VDP logon with SCA/SCABR is not working when assigned to a soft key.

- A SIP outbound proxy address must be assigned in the startup.cfg file, that is, the SIP outbound proxy address is the local address of the EX-Controller / GX-Gateway.

Setting up MX-ONE for GX Controller

Number Analysis

Number Analysis Data

Type of Series	**Number Series**
Extension Number Series	10000 - 31999 33200 - 49999 67000 - 67999
External Destination Code	068 081 – 088 321 331 81 - 88
LCR Access Code	00

Call Discrimination Data

Type of Series	**Number Series**
External/Internal Number	CDCAT Customer
Number Analysis Data	

Extension Data

Figure 11.2: Directory Number Profile

```
Dir    Cust  Lim  Csp Feature  Lang  Max  Secretary  Max  Security  AMC  Video BluStar     Third
Party  Csta   Free On     Hotline  Hotline Num  Backup Num         Area
                    level              Cost             Term Exception            Client Mod   SIP
Client  Supp  Second Line                                            Code
11101  0   1   9            -   -   No       1    Yes    No   No   -                No
00     1          -     -           08101344311101    013
11102  0   1   9            -   -   No       1    Yes    No   No   -                No
00     1          -     -           08101344311102    013
11103  0   1   9            -   -   No       1    Yes    No   No   -                No
00     0          -     -           08101344311103    013
11104  0   1   9            -   -   No       1    Yes    No   No   -                No
00     0          -     -            -          -
11105  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08101344311105    013
11106  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08101344311106    013
22101  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08203132522101   031
22102  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08203132522102   031
22103  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08203132522103   031
22104  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08203132522104   031
22105  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08203132522105   031
22106  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -           08203132522106   031
67820  0   1   11           -   -   No       4    Yes    No   No   -                No
00     1          -     -            -          -
67821  0   1   9            -   -   No       4    Yes    No   No   -                No
00     0          -     -            -          -
67822  0   1   9            -   -   No       1    Yes    No   No   -                No
00     1          -     -            -          -
```

MDSH>

Common Service Profile 9:

Cust: 0

Traf : 0103151515

Serv: 11110001100100000000100000300

Cdiv: 111000111010000

Roc: 000001

Npres: 0011000

Offered Time: 0

Forced DisconnectTime: 0

CnnLog: 0

Csp Name: Standard

Common Service Profile 11:

Cust: 0

Traf : 0103151515

Serv: 11113001100100000000100000300

Cdiv: 111000111010000

Roc: 000001

Npres: 0011000

Offered Time: 0

Forced DisconnectTime: 0

CnnLog: 0

Csp Name: Intrusion

Least Cost Routing Data

Least Cost Destination Data

Table 11.1: External Number Table

Entry	TRC	PRE	Conf
00013443111	8		N
00031325	8		N
00040598	8		N
00084226	7		N
000856867	7		N

END

Least Cost Destination Data

Table 11.2: Number Length Table

Entry	TRC	PRE	CONF	MIN	MAX	ACF
001	0		N	6	18	Y
002	0		N	6	18	Y
003	0		N	6	18	Y
004	0		N	6	18	Y
005	0		N	6	18	Y
006	0		N	6	18	Y
007	0		N	6	18	Y
008	0		N	6	18	Y
009	0		N	6	18	Y

Least Cost Destination Data

Table 11.3: Number Table

Entry	TRC	PRE	ACCT	FRCT	TOLL	CBCS	BTON	TNS	OSA
	5		0	1	1111111 1111111 1		0		
	5		0	2	1111111 1111111 1		0		
	5		0	3	1111111 1111111 1		0		
	4		0	4	1111111 1111111 1		0		

END

Least Cost Destination Data

Table 11.4: Fictitious Destination Table

FRCT	TZONE	PRE
1	1	081
2	1	083
3	1	085
4	1	088

END

Route Data

ROCAP

Route Category Data

Figure 11.3: Route Category Data

```
ROU        CUST SEL          TRM SERV      NODG DIST  DISL TRAF      SIG
BCAP
81          7110000000000010  4    3100000001  0    30    128  03151515 0111110000A0
001100
83          7110000000000010  4    3100000001  0    30    128  03151515 0111110000A0
001100
211         7110000000000010  4    3100000001  0    30    128  03151515 0111110000A1
001100
```

RODAP

Route Data

Table 11.5: Route Data

ROU	Type	VARC	VARI		VARO	Filter
81	TL66	H'00000000	H'0000000 0	H'00000000	NO	
83	TL66	H'00000000	H'0000000 0	H'00000000	NO	
211	TL66	H'00000000	H'0000000 0	H'00000000	NO	

SIP ROUTE

One SIP route to each branch node is specified.

Route 81 towards BO#1 (Linköping)

route : 81

protocol = tcp

profile = Default

service = PUBLIC

uristring0 = sip:?@192.168.17.81

fromuri0 = sip:?@192.168.17.44

remoteport = 5070

accept = TRUNK_INFO

match = user=trunk

register = NO_REG

Route 83 towards BO#2 (Göteborg)

route : 83

protocol = tcp

profile = Default

service = PUBLIC

uristring0 = sip:?@192.168.17.83

fromuri0 = sip:?@192.168.17.44

remoteport = 5070

accept = TRUNK_INFO

match = user=trunk

register = NO_REG

Route 211 towards BO#3 (Malmö)

route : 211

protocol = udp

profile = MXONE-tieline

service = PRIVATE_SERVICES

uristring0 = sip:?@192.168.17.94;tgrp=BO3

fromuri0 = sip:?@192.168.17.44;tgrp=BO3

accept = ALL

register = SET_BY_PROFILE

trusted = TRUST_BY_PROFILE

NOTE: BO#3 is only reached by SIP trunks as it is an EX controller system running an own instance of MX-ONE.

Setting up the GX Gateway

This section describes how to setup BO#1 (Linköping).

Setting up BO#2 (Göteborg) is similar, only numbering information and own IP-address is changed.

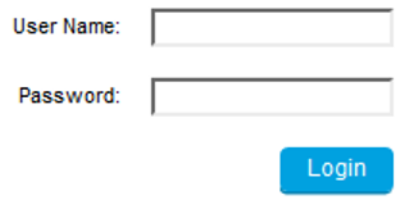
Logon

This section describes how to setup BO#1.

Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network).

NOTE: If DHCP is not running into the network then, plug in the network cable to the ETH2 port on EX Controller and use the default IP address of 192.168.0.10 to open the EX Controller Interface.

Figure 11.4: Login page



This section describes how to setup BO#1.

1. Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network)
   – User name/password: public /
   – User name/password: admin/administrator
2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.
3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

Network Settings

Host

1. Select **Network** > **Host** and keep the default configuration interface as mentioned below.

Figure 11.5: Host settings - 1

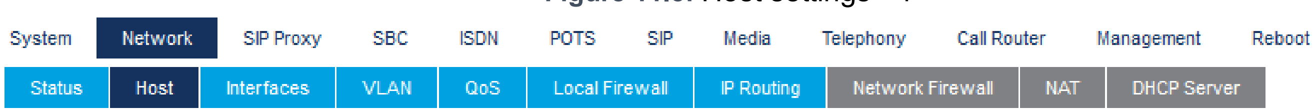
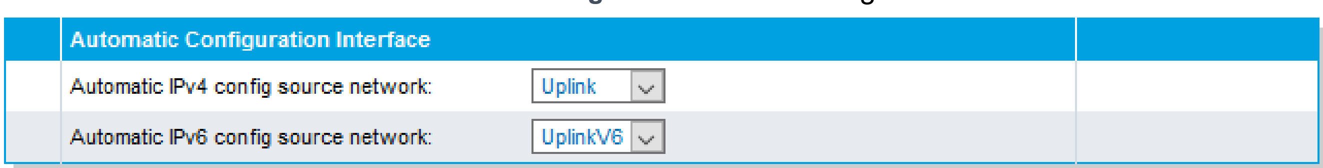
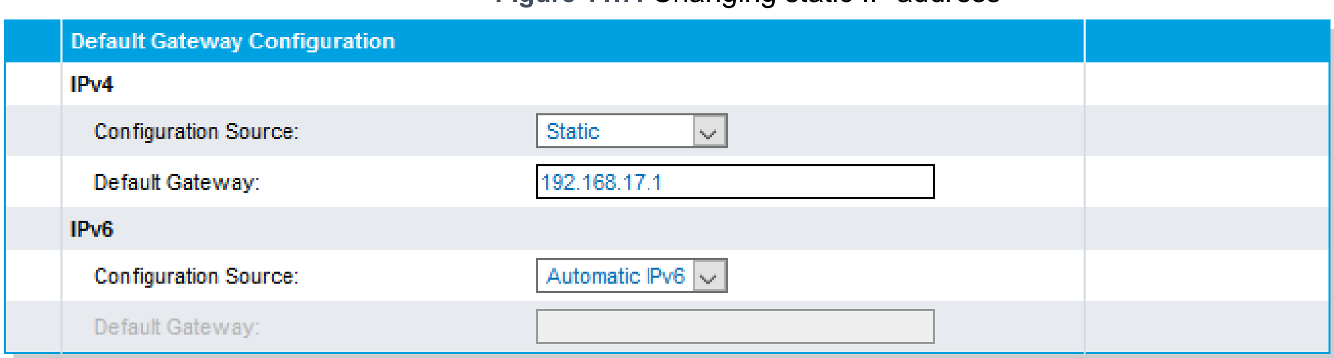


Figure 11.6: Host settings - 2



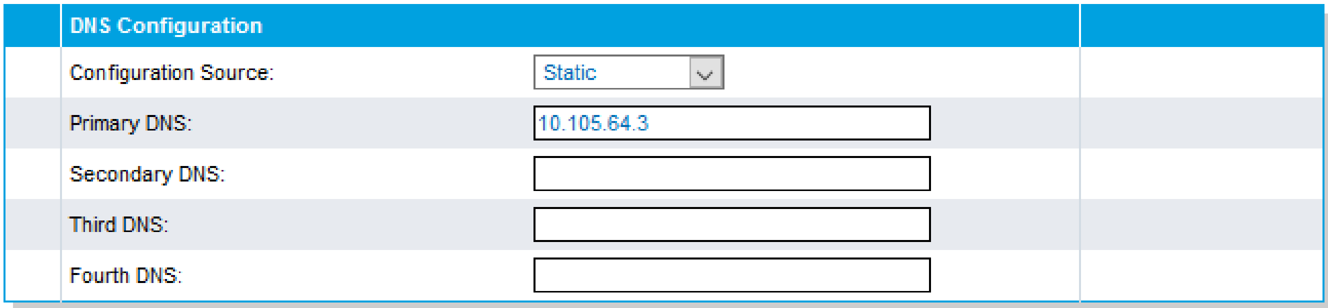
2. Change to **Static IP-address** and enter default Gateway (GW).

Figure 11.7: Changing static IP address



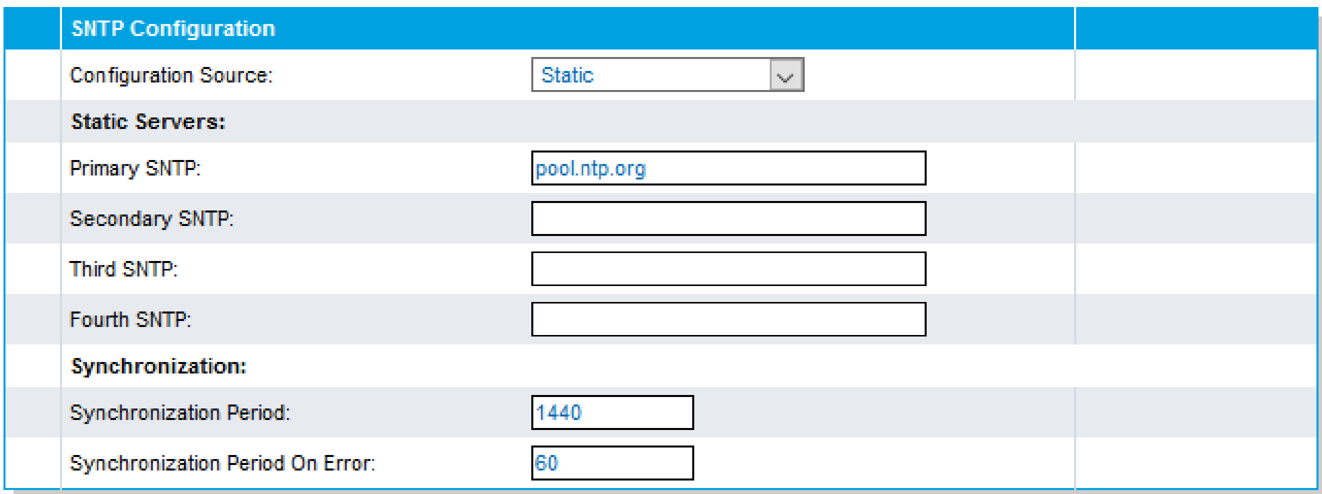
3. Change to static DNS server and enter IP-address or FQDN to DNS server.

Figure 11.8: Changing static DNS server



4. Change to static SNTP server, enter time server data.

Figure 11.9: Changing to static SNTP server

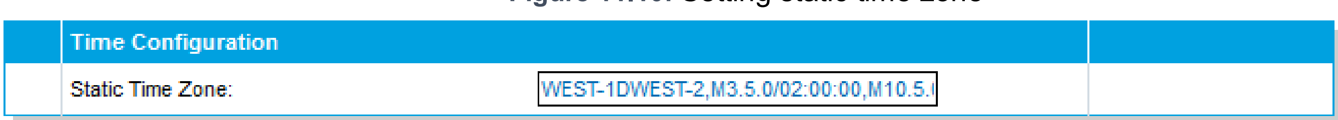


5. Set the **Static Time Zone**.

   Valid options are:

- Pacific Time (Canada and US): PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
- Mountain Time (Canada and US): MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
- Central Time (Canada and US): CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
- Eastern Time (Canada and US): EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
- Atlantic Time (Canada): AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
- GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
- W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
- China Standard Time: CST-8
- Tokyo Standard Time: TST-9
- Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
- Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
- UTC (Coordinated Universal Time): UTC0

Figure 11.10: Setting static time zone



6. Leave all other items as it is and click **Apply** when finished.

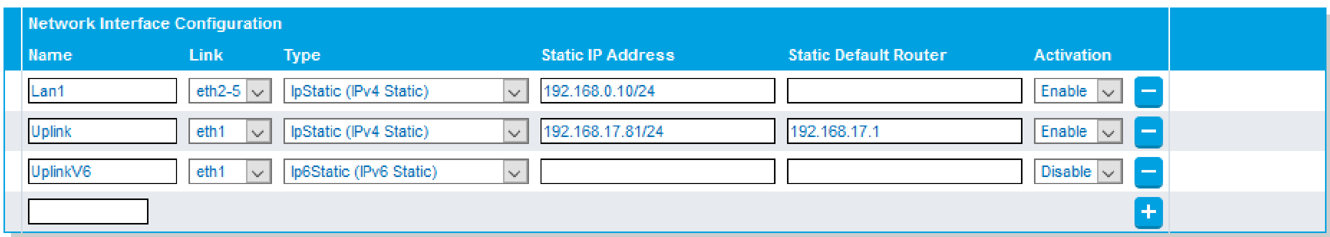
Interfaces

1. Go to **Network** > **Interface**.

Figure 11.11: Interface

2. Change **Uplink** to **IpStatic (IPv4 Static)** and enter the static IP-address and Static Default Gateway.

Figure 11.12: Changing Uplink to IpStatic



3. Leave all other items as it is and click Apply when ready.

   NOTE: When the IP-address is changed the connection is lost and a new logon must be done with the new IP-address.

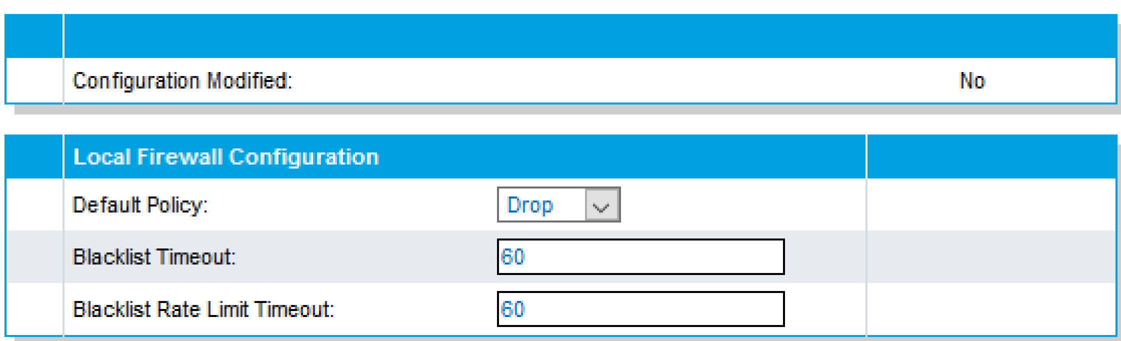
Local Firewalls

1. Go to **Network** > **Local Firewall**.

Figure 11.13: Local firewalls

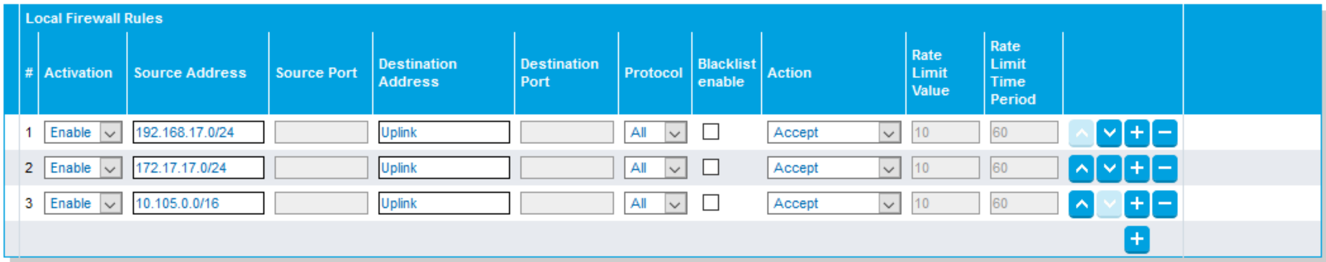
2. If local firewall security is needed change default policy to **Drop**.

Figure 11.14: Changing default policy



3. Enter the networks for which traffic can enter from.

Figure 11.15: Enter network traffic



Local Firewall Rules

#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period
1	Enable	192.168.17.0/24		Uplink		All	☐	Accept	10	60
2	Enable	172.17.17.0/24		Uplink		All	☐	Accept	10	60
3	Enable	10.105.0.0/16		Uplink		All	☐	Accept	10	60

4. Click **Save** or **Save and Apply** when ready.

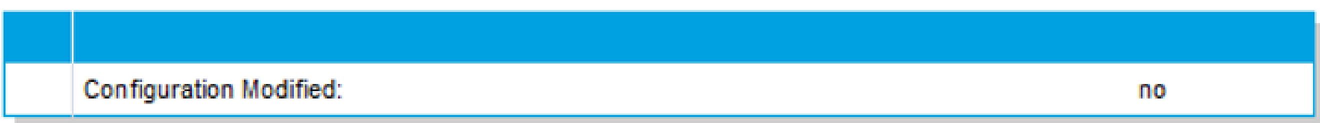
Session Board Controller (SBC)

Configuration

1. Go to **SBC** > **Configuration**. The following Call Agents are present.

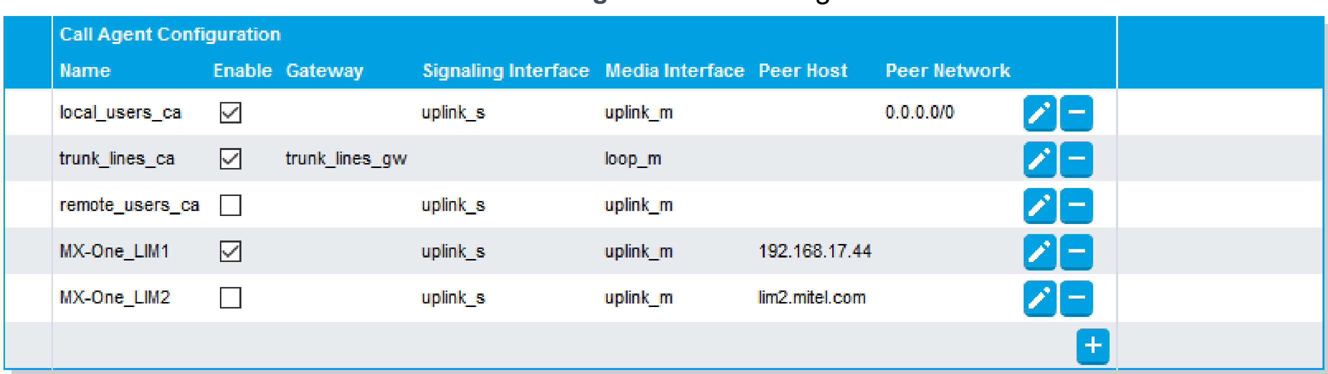
Figure 11.16: Call agent - 1

Figure 11.17: Call agent - 2



Configuration Modified:	no

Figure 11.18: Call agent - 3

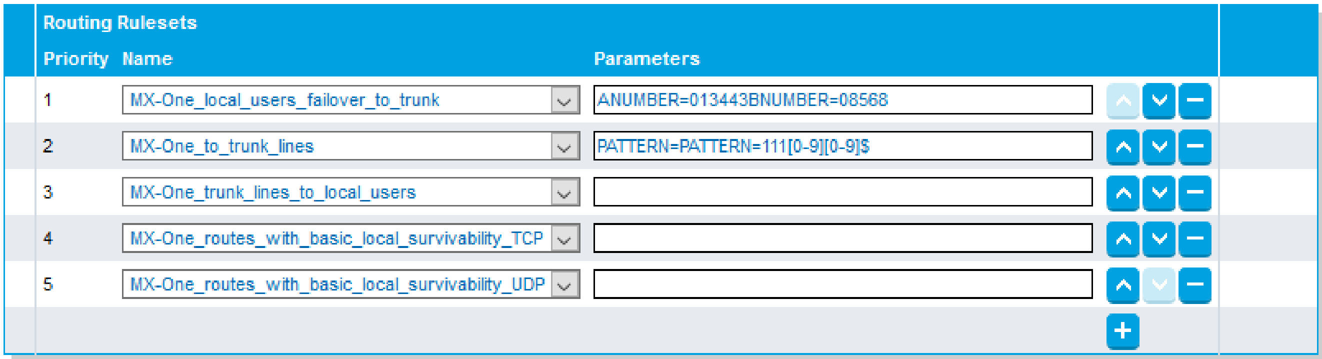


Call Agent Configuration

Name	Enable	Gateway	Signaling Interface	Media Interface	Peer Host	Peer Network
local_users_ca	☑		uplink_s	uplink_m		0.0.0.0/0
trunk_lines_ca	☑	trunk_lines_gw		loop_m		
remote_users_ca	☐		uplink_s	uplink_m		
MX-One_LIM1	☑		uplink_s	uplink_m	192.168.17.44	
MX-One_LIM2	☐		uplink_s	uplink_m	lim2.mitel.com	

2. Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers in when the GW is in survivable mode, that is, the call is routed to PSTN and thus needs to be prefixed.
3. Enter the number range that is allowed in the branch in the `PATTERN` parameter. For example, 111[0-9][0-9]$ means that the allowed number range in this branch is 11100 – 11199.

Figure 11.19: Parameters screen



4. Configure each call agent (ca).

5. Click to enter specific data for each call agent.

Local_users_ca

- Enter the IP-address of MX-ONE to the DOMAIN variable.
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 111[0-9][0-9]$ means that the allowed number range in this branch is 11100 – 11199.
- Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers in when the GW is in survivable mode, that is, the call is routed to PSTN and thus needs to be prefixed.

Figure 11.20: Configure Call Agent screen

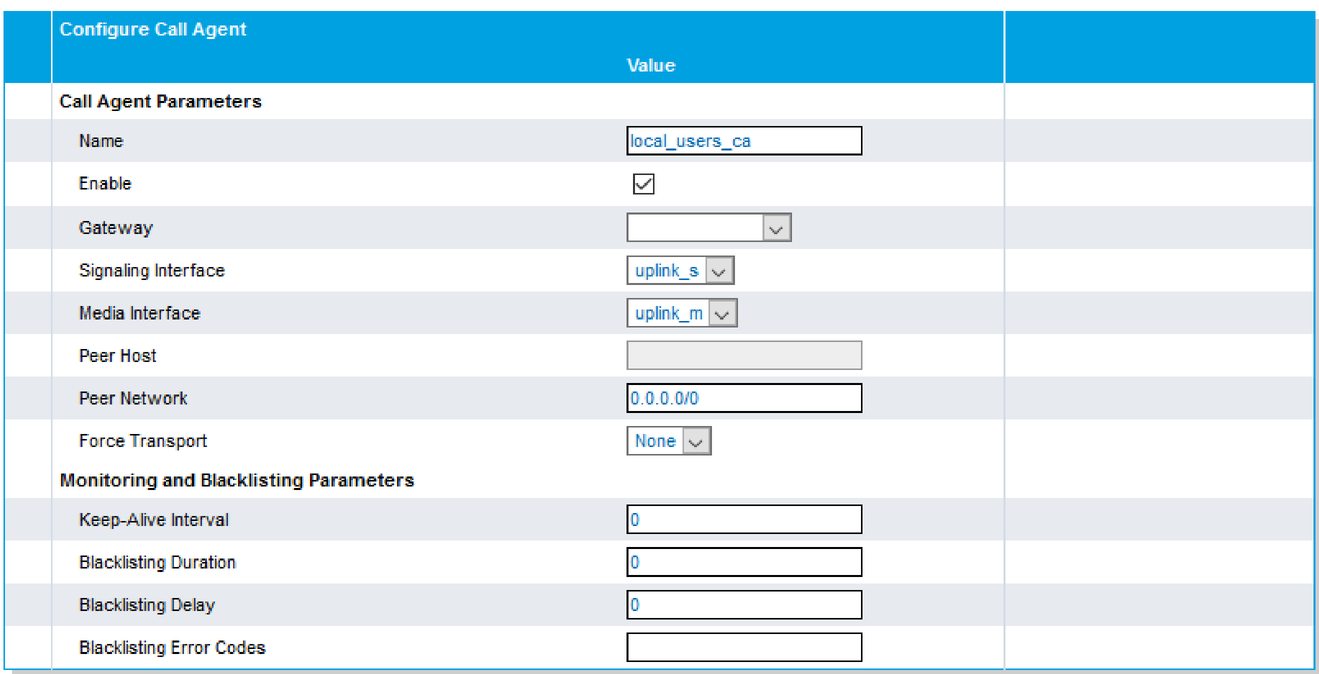
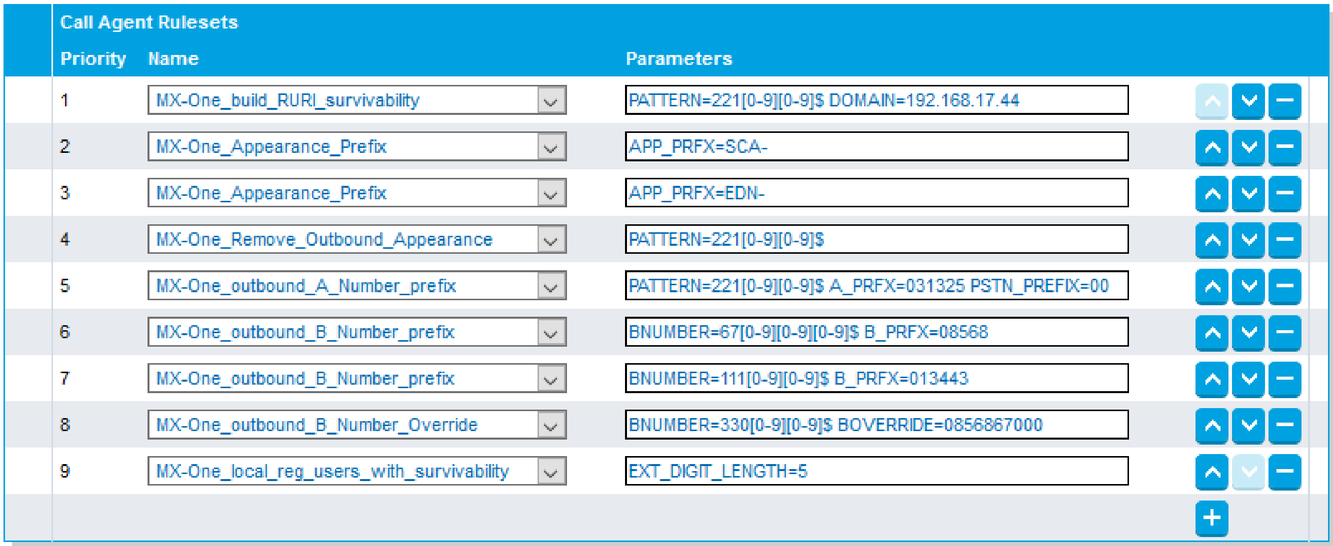


Figure 11.21: Call Agent Rulesets screen



Ruleset MX-ONE_build_RURI survivability (ACTIVE ONLY IN SURVIVAL MODE)

PATTERN=111[0-9][0-9]$

The pattern for the internal range of numbers, in this example the internal range would be 11100 – 11199

Calls to this number range stay always local (do not send to the PSTN in survival mode)

DOMAIN=192.168.17.44

The IP of the headquarter (the main PBX), in this case 192.168.17.44

Ruleset: MX_ONE_Appearance_Prefix (ACTIVE ONLY IN SURVIVAL MODE)

NEW: APP_PREFIX=SCA-

This is the prefix for the usernames connected with shared appearance. In this example we have two: “SCA-“ and “EDN-“

Ruleset: MX-ONE_Remove_Outbound_Appearance (ACTIVE ONLY IN SURVIVAL MODE)

PATTERN=111[0-9][0-9]$

This rule will remove any prefix used for Shared Call Appearance. The pattern for the internal range of numbers, in this example the internal range would be 11100 – 11199

Ruleset: MX-ONE_outbound_A_Number_prefix (ACTIVE ONLY IN SURVIVAL MODE)

PATTERN=111[0-9][0-9]

This defines the local numbers.

A_PRFX=013443

This is the prefix for the local numbers used on outgoing calls to the PSTN (in this example we received a number block 013443xxxxx from the PSTN provider and add the prefix on outgoing calls, so that the calling party number sent to the PSTN is correct)

PSTN_PREFIX=00

Dial this prefix to break out to the PSTN. Here we have configured the “00” (not to be mixed up with the “00” for international calls!)

Ruleset: MX-ONE_outbound_B_Number_prefix (ACTIVE ONLY IN SURVIVAL MODE)

This ruleset applies to calls to numbers defined in BNUMBER and will add B_PRFX to the called party number.

BNUMBER=67[0-9][0-9]$

Applies to calls to the specific range of extensions,

B_PRFX=08568

This is the prefix for the Called Party Number. In this case it was build like: National Prefix (08) + Main part of the HQ’s local number: (568), in case somebody dials an extension in the HQ

Ruleset: MX-ONE_outbound_B_Number_Override (ACTIVE ONLY IN SURVIVAL MODE)

This ruleset applies to calls to numbers defined in BNUMBER and will use the BOVERRIDE as Called Party Number.

BNUMBER=330[0-9][0-9]$

Applies to calls to the specific range

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE, in this example they will be sent to 0856867000

Ruleset: MX-ONE_local_reg_users_with_survivability

(Builds the registration cache for survivability purpose)

EXT_DIGIT_LENGTH=5

The length of the internal numbers, in this case set to “5”, for numbers like “00001 – 99999”

1. Click **Save** when done.

Trunk _ Lines _ca

- Enter the IP-address of MX-ONE to the DOMAIN variable (in two places).
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 111[0-9][0-9]$ means that the allowed number range in this branch is 11100 – 11199.
- Insert a main extension number in MAIN_EXT parameter, this is could be the local answering position when dialling a vacant number, and so on.
- Enter the PSTN_PREFIX and STRIPNDIGTS, this is used to remove the public access code when dialling PSTN calls in survivable mode.

Figure 11.22: Trunk_Lines_ca

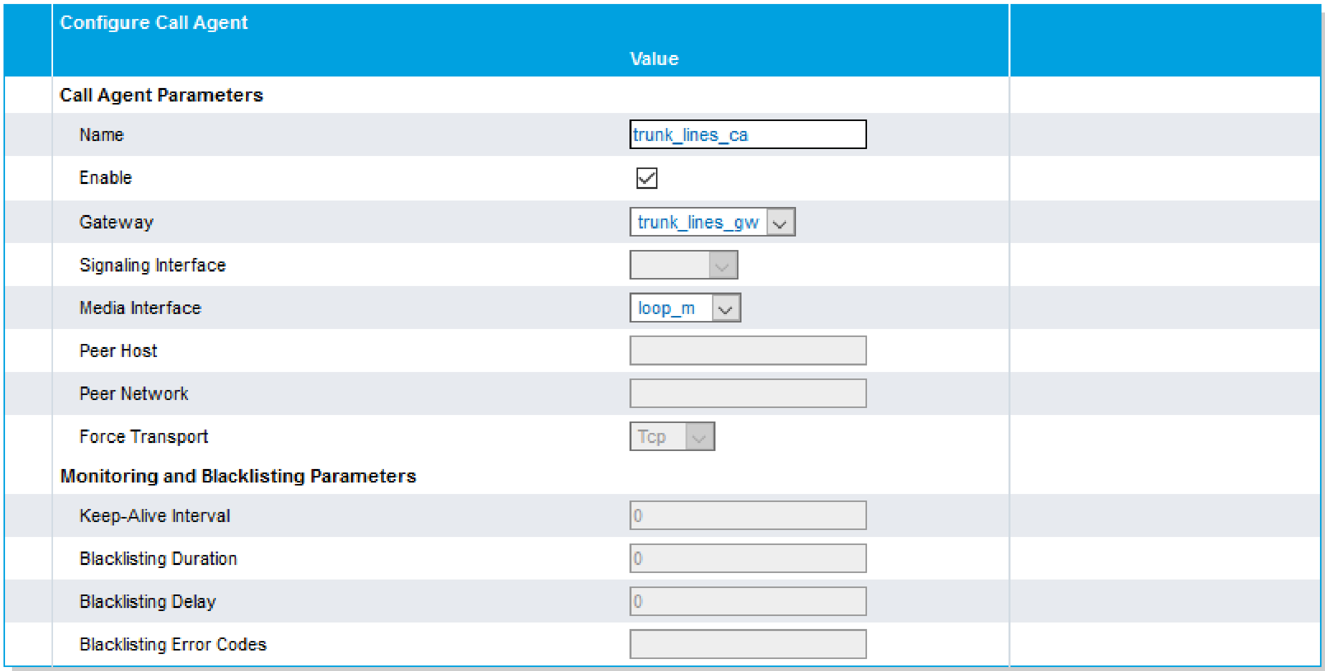
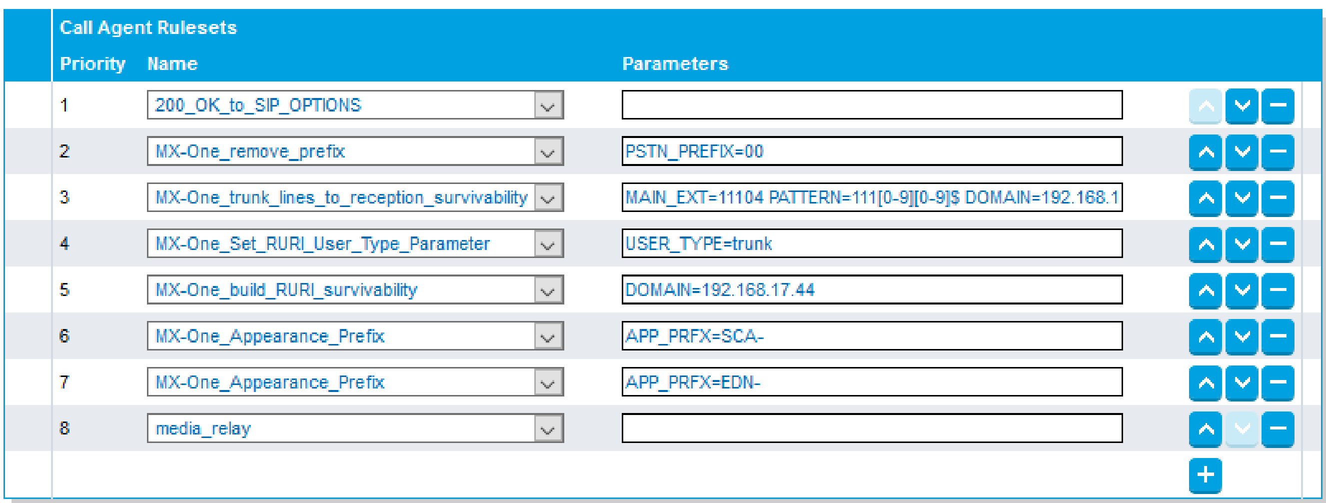


Figure 11.23: Trunk_Lines_ca Parameters



Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This is the prefix used to dial out to the PSTN

Ruleset: MX-One_trunk_lines_to_reception_survivability

An incoming call in survival mode will be sent to MAIN_EXT destination if not reachable

MAIN_EXT=11104

This will receive the incoming call in case the original destination is not reachable (not defined or not registered)

PATTERN=111[0-9][0-9]$

The pattern for the internal range of numbers, in this example the internal range would be 11100 – 11199

DOMAIN=192.168.17.44

The IP of the headquarter (the main PBX), in this case 192.168.17.44

Ruleset: MX-One_Set_RURI_User_Type_Parameter

Set RURI User Type Parameter

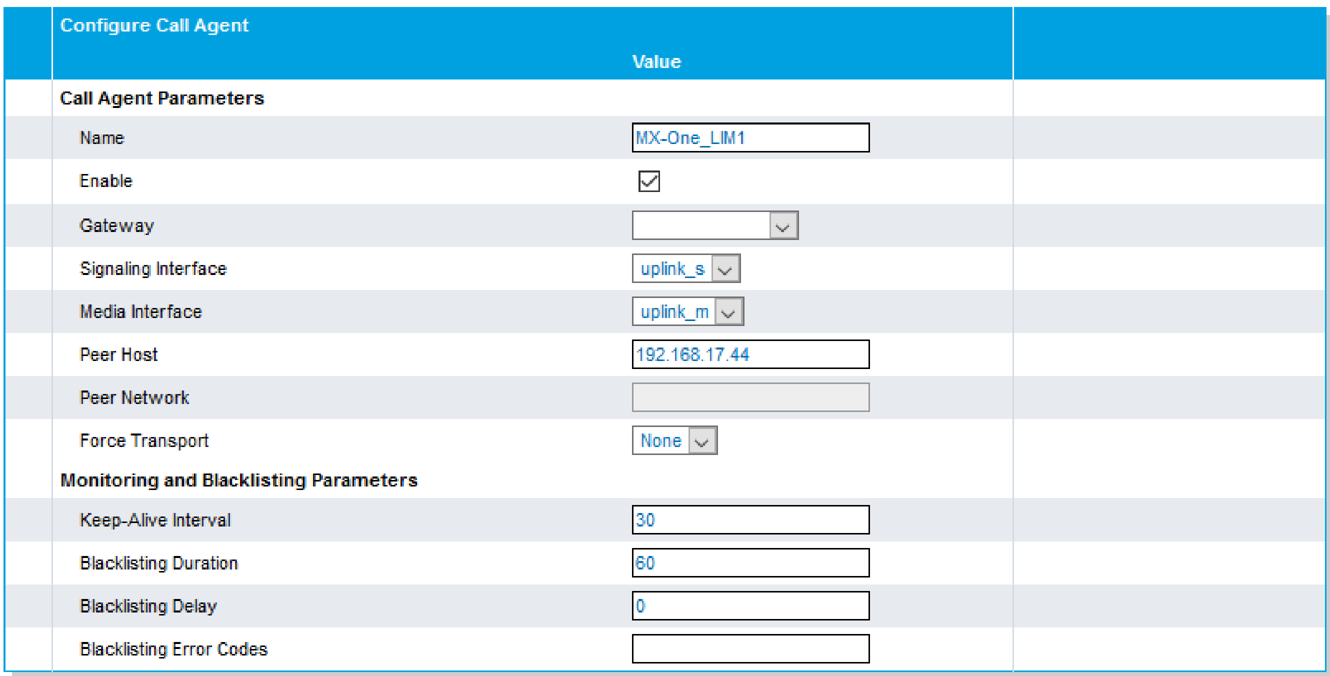
USER_TYPE=trunk

1. Click Save when done.

MX-ONE_Lim1

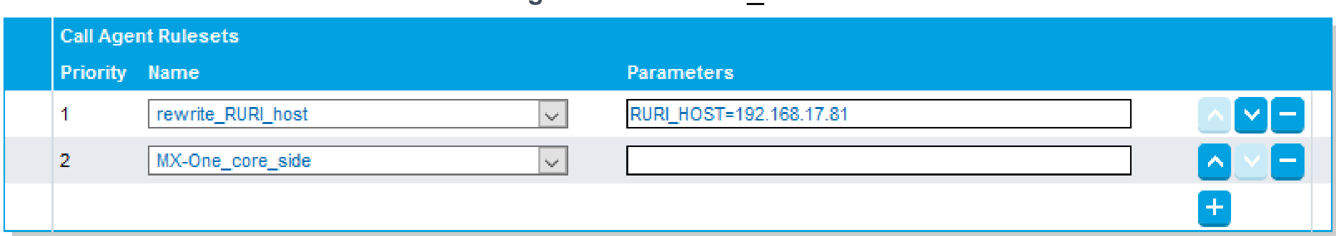
1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 11.24: Peer Host field



2. Enter the IP-address of the GW in the **RURI_HOST** parameter.

Figure 11.25: RURI_HOST Parameter



Ruleset: rewrite_RURI_host
Customize RURI host
RURI_HOST= 192.168.17.81. This is the local IP address.

3. When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.
4. Click **Save** when ready.

MX-ONE_TRUNK

1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 11.26: MX-ONE Trunk

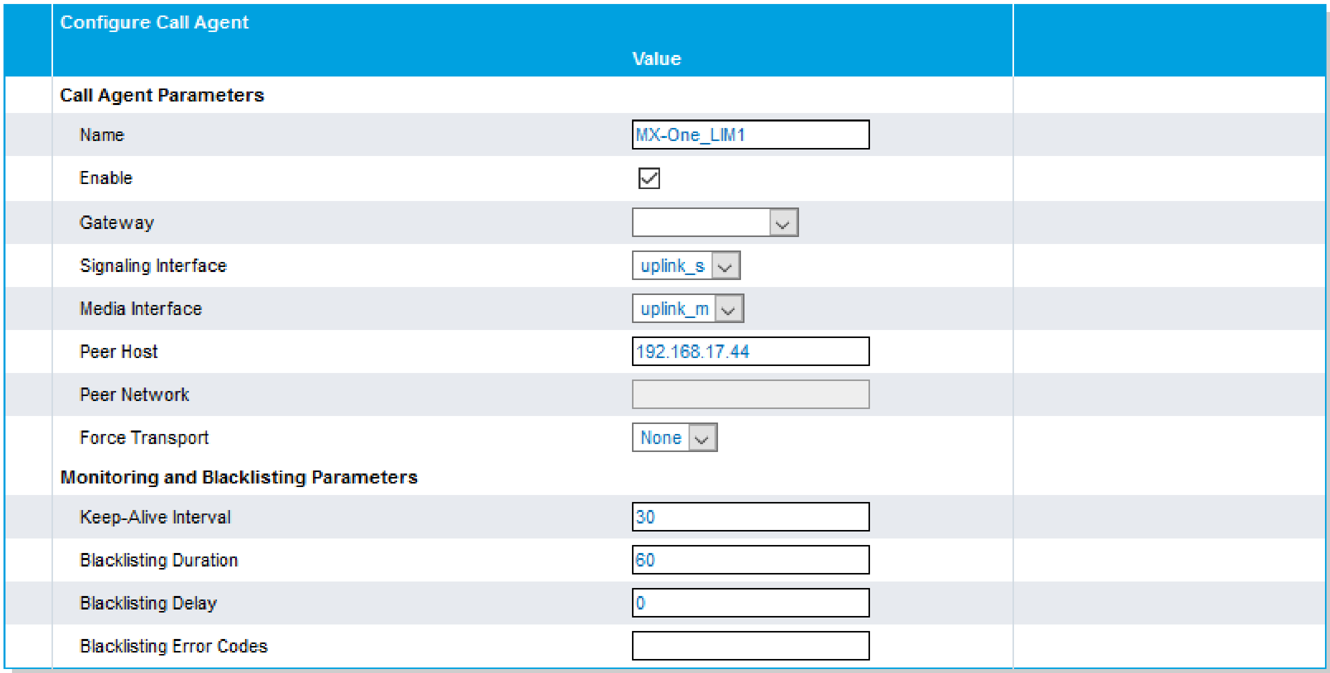
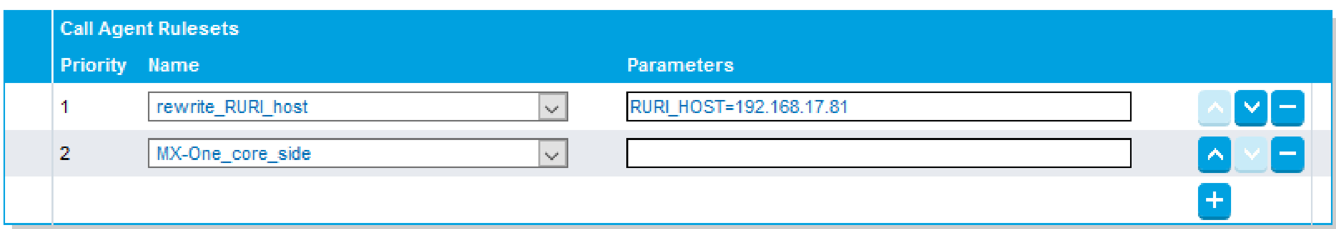


Figure 11.27: MX-ONE_TRUNK Parameters



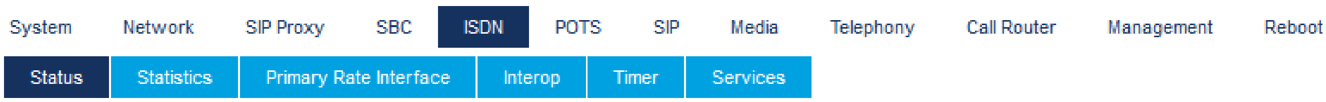
2. When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.
3. Click **Save** when ready.

Figure 11.28: Configuration Modified

4. If the indication is not removed there are some error in the configuration.
5. Double check changes described above and correct them.

ISDN

Figure 11.29: ISDN tab



If ISDN trunks are used, press **Start Sensing**. The system automatically detects certain parameters, for example, number of channels.

Primary Rate Interface

Figure 11.30: Primary Rate Interface

1. When sensing is done for several markets, specific parameters can be changed.

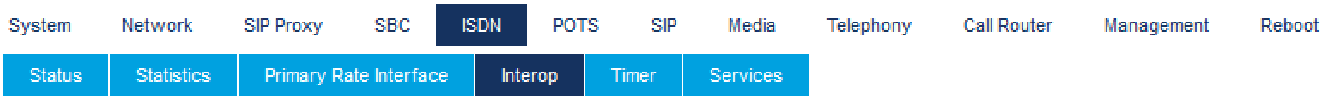
Figure 11.31: Interface Configuration

Interface Configuration	
Line Type: [Configure]	E1
Endpoint Type:	TE
Clock Mode:	Slave
Port Pinout:	Auto
Monitor Link State:	Enable
Line Coding:	HDB3
Line Framing:	CRC4
Signaling Protocol:	DSS1
Network Location:	User
Preferred Encoding Scheme:	G.711 a-Law
Fallback Encoding Scheme:	G.711 u-Law
Channel Range:	1-30
Channels Reserved for Incoming Calls:	
Channels Reserved for Outgoing Calls:	
Channel Allocation Strategy:	Ascending
Maximum Active Calls:	30
Signal Information Element:	Disable
Inband Tone Generation:	Enable
Inband DTMF Dialing:	Enable
Overlap Dialing:	Disable
Calling Name Max Length:	34
Exclusive B-Channel Selection:	Disable
Sending Complete:	Enable
Send Restart On Startup:	Enable
Link Establishment:	Permanent
Accepted Status Causes:	
Accepted Progress Causes:	1-127
Send Isdn Progress:	Send All
Send Progress Indicator IE:	Send All
Default TON for Calling Party Number IE:	National
Default NPI for Calling Party Number IE:	Isdn Telephony
Default PI for Calling Party Number IE:	Presentation Allowed
Default SI for Calling Party Number IE:	Context Dependent
Default TON for Called Party Number IE:	National
Default NPI for Called Party Number IE:	Isdn Telephony
Notification User Suspended:	Ignore

2. Click **Apply** and restart requested service when done.

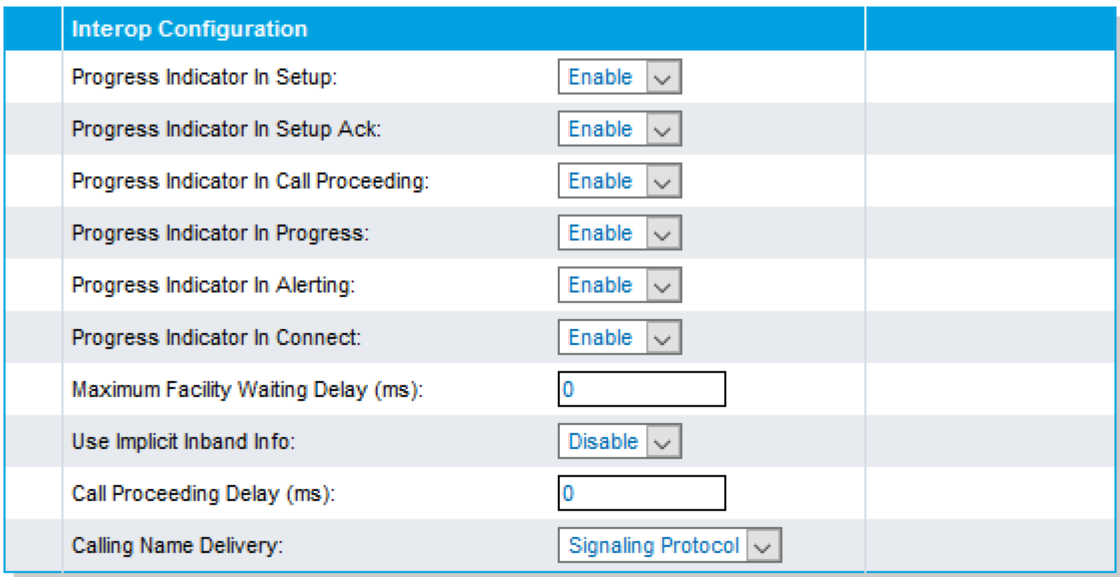
Interop

Figure 11.32: Interop



1. You can change other parameters dependent on market.

Figure 11.33: Interop Configuration screen



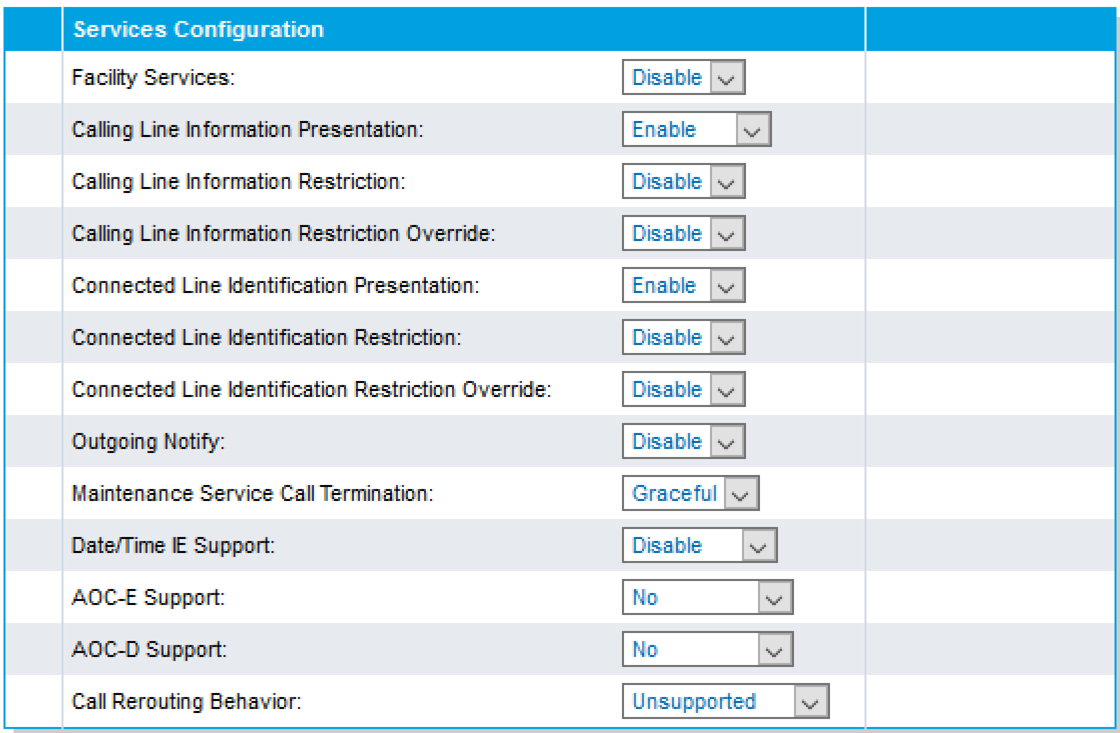
2. Click **Apply** and restart requested service when done.

Services

Figure 11.34: Services

1. Change other parameters dependent on market.

Figure 11.35: Services Configuration screen



2. Click **Apply** and restart requested service when done.

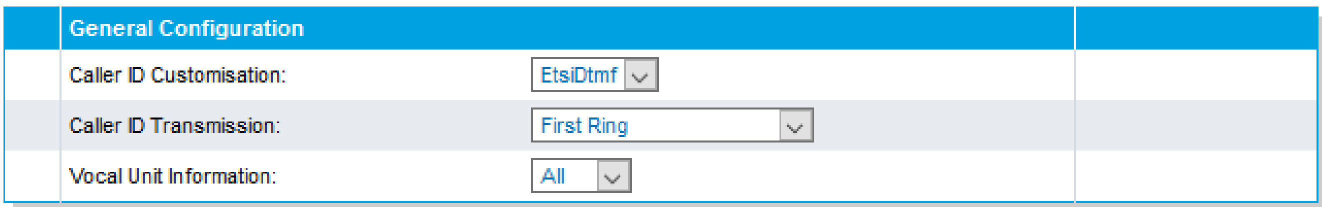
POTS

Config

Figure 11.36: Config

1. Set market specific data for Caller Id handling.

Figure 11.37: General Configuration screen



2. Click **Apply** when done and restart service.

FXS Configuration

Figure 11.38: FXS Configuration

1. Set analog phone specific data according to market.

Figure 11.39: FXS Configuration screen

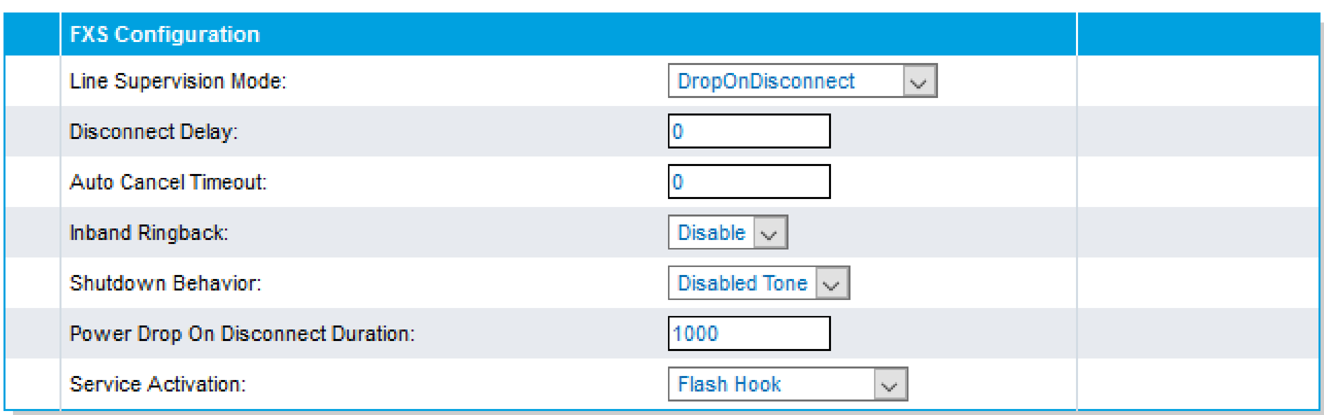
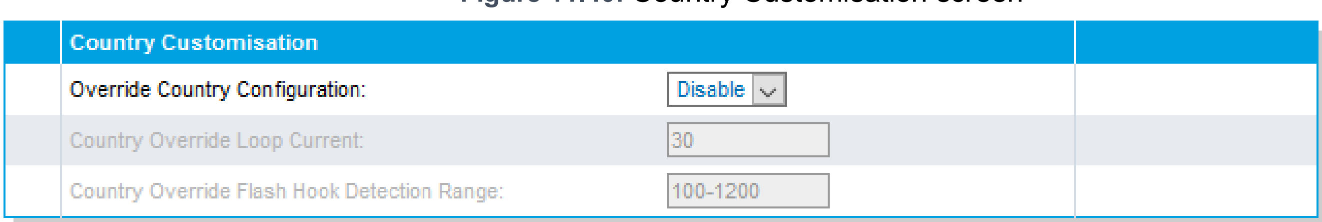


Figure 11.40: Country Customisation screen



2. Click **Apply** when done and restart service.

SIP

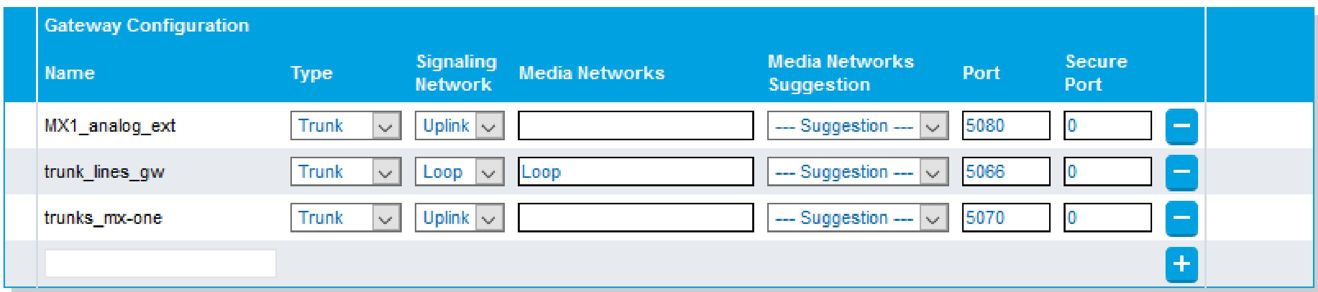
Gateways

Following gateways and port numbers are pre-defined.

Figure 11.41: Gateways

NOTE: A SIP route must be defined in MX-ONE to handle traffic to and from the ‘trunks_MX-ONE’ gateway.

Figure 11.42: trunks_mx-one



Gateway Configuration

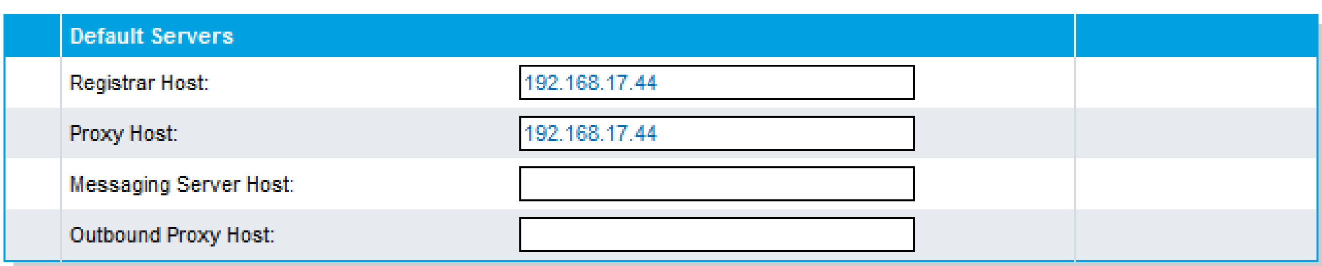
Name	Type	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port
MX1_analog_ext	Trunk	Uplink		--- Suggestion ---	5080	0
trunk_lines_gw	Trunk	Loop	Loop	--- Suggestion ---	5066	0
trunks_mx-one	Trunk	Uplink		--- Suggestion ---	5070	0

Servers

Figure 11.43: Servers

1. Enter IP-address to MX-ONE in both **Registrar Host** and **Proxy Host** fields.

Figure 11.44: Default Servers



Default Servers	
Registrar Host:	192.168.17.44
Proxy Host:	192.168.17.44
Messaging Server Host:	
Outbound Proxy Host:	

2. Change **trunk_lines_gw** to **Yes** in the drop-down list for **Gateway Specific**.

Figure 11.45: trunk_lines_gw

Registrar Servers		
Gateway	Gateway Specific	Registrar Host
MX1_analog_ext	No	192.168.0.10:0
trunk_lines_gw	Yes	%sbc%
trunks_mx-one	No	192.168.0.10:0

3. Enter IP-address of MX-ONE in the **Proxy Host** field.
4. Enter IP-address of the gateway in the **Outbound Proxy Host** field.

Figure 11.46: Outbound Proxy Host field

Proxy Servers			
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
MX1_analog_ext	Yes	192.168.17.44	192.168.17.81
trunk_lines_gw	Yes	%sbc%	%sbc%
trunks_mx-one	No	192.168.0.10:0	0.0.0.0:0

5. Enter the IP-address of the gateway as **Alternate Destination** for **MX1_analog_ext**.
6. Enter the IP-address of MX-ONE as Alternate Destination for trunks_mx-one.

Figure 11.47: Alternate Destination for trunks_mx-one

Keep Alive Destination	
Gateway	Alternate Destination
MX1_analog_ext	192.168.17.81
trunk_lines_gw	127.0.0.1
trunks_mx-one	192.168.17.44

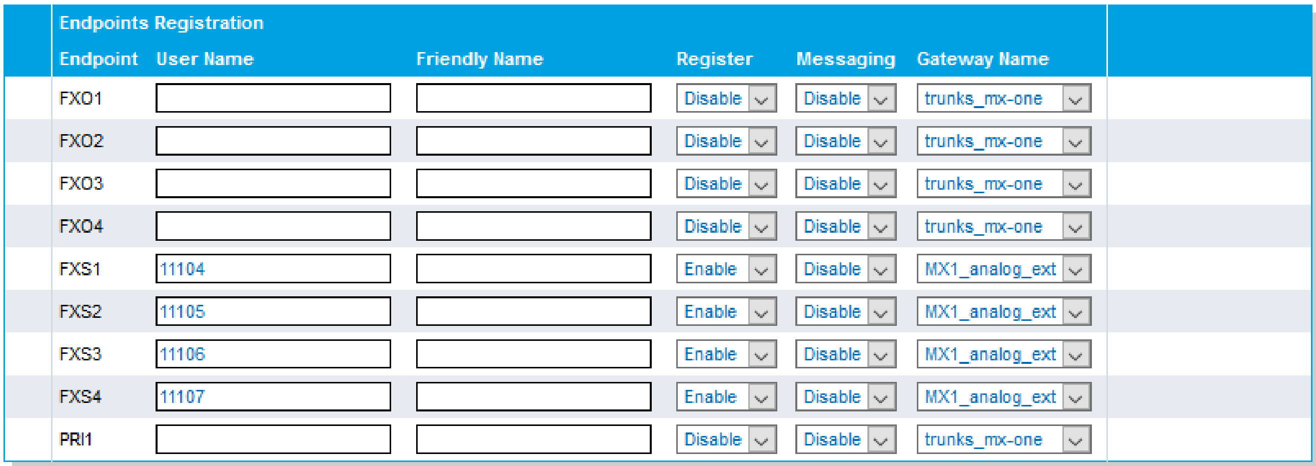
7. Click **Apply** when done and restart service.

Registrations

Figure 11.48: Registrations

1. Enter the extension numbers for the analog extensions.

Figure 11.49: Endpoints Registration screen



Endpoints Registration

Endpoint	User Name	Friendly Name	Register	Messaging	Gateway Name
FXO1			Disable	Disable	trunks_mx-one
FXO2			Disable	Disable	trunks_mx-one
FXO3			Disable	Disable	trunks_mx-one
FXO4			Disable	Disable	trunks_mx-one
FXS1	11104		Enable	Disable	MX1_analog_ext
FXS2	11105		Enable	Disable	MX1_analog_ext
FXS3	11106		Enable	Disable	MX1_analog_ext
FXS4	11107		Enable	Disable	MX1_analog_ext
PRI1			Disable	Disable	trunks_mx-one

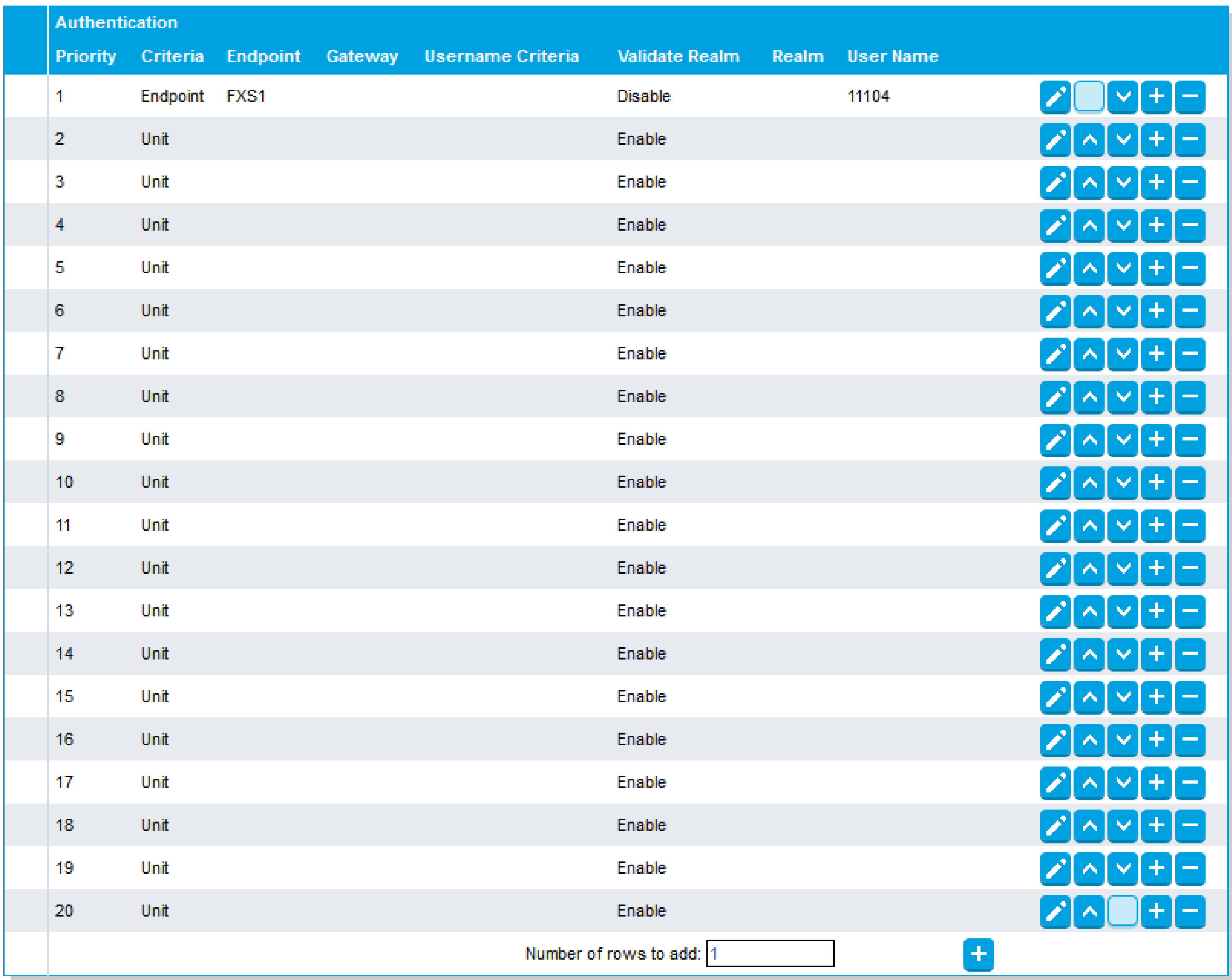
2. Click **Apply** or **Apply and Refresh** when done.

Authentication

Figure 11.50: Authentication

1. If password is required press for any item.

Figure 11.51: Authentication Screen



Authentication

Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name
1	Endpoint	FXS1			Disable		11104
2	Unit				Enable		
3	Unit				Enable		
4	Unit				Enable		
5	Unit				Enable		
6	Unit				Enable		
7	Unit				Enable		
8	Unit				Enable		
9	Unit				Enable		
10	Unit				Enable		
11	Unit				Enable		
12	Unit				Enable		
13	Unit				Enable		
14	Unit				Enable		
15	Unit				Enable		
16	Unit				Enable		
17	Unit				Enable		
18	Unit				Enable		
19	Unit				Enable		
20	Unit				Enable		

Number of rows to add: 1

2. Indicate for which Endpoint and Criteria the changes are to apply.
3. Enter the Auth Code, in the **Password** field.
4. In the **Validate Realm** field, select **Disable**.

Figure 11.52: Validate Realm field

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Endpoint	FXS1			Disable		11104	********

5. Click **Apply** or **Apply and Refresh Registration** when done and restart service. The result after 'Registration' and 'Authentication' should be like as follows:

Figure 11.53: Endpoints Registration Status

Endpoints Registration Status				
Endpoint	User Name	Gateway Name	Registrar	Status
FXS1	11104	MX1_analog_ext	192.168.17.44:0	Registered
FXS2	11105	MX1_analog_ext	192.168.17.44:0	Registered
FXS3	11106	MX1_analog_ext	192.168.17.44:0	Registered

Transport

Figure 11.54: Transport

1. Enable UDP if required.

Figure 11.55: Protocol Configuration screen

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable		Enable		Disable	

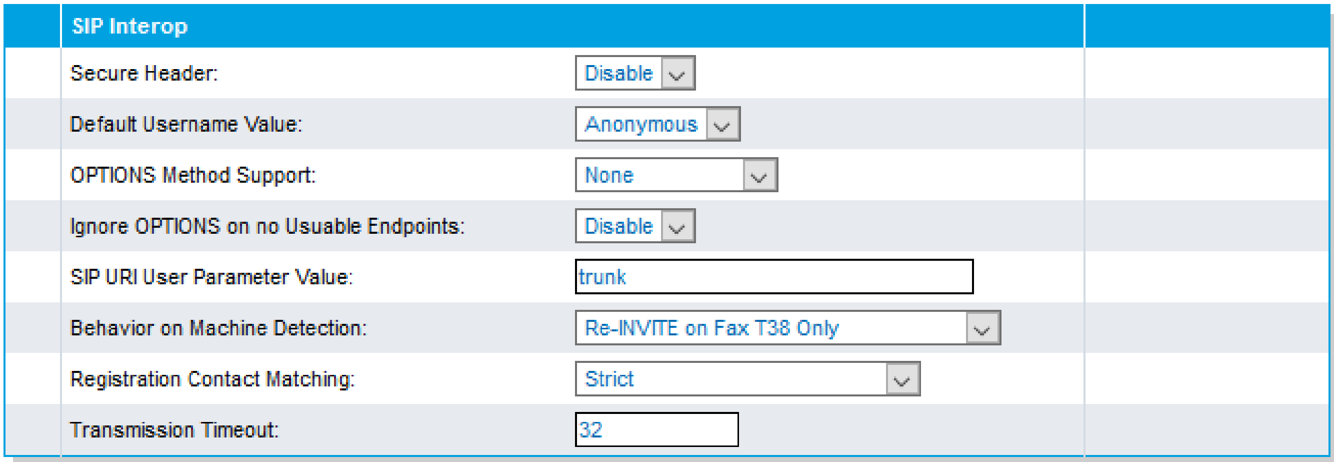
2. Click **Apply** when done and restart service.

Interop

Figure 11.56: Interop

1. Select **trunk** in the **SIP URI User Parameter Value** field.
2. This is used in the 'match' parameter for the SIP route in MX-ONE.

Figure 11.57: SIP URI User Parameter Value field



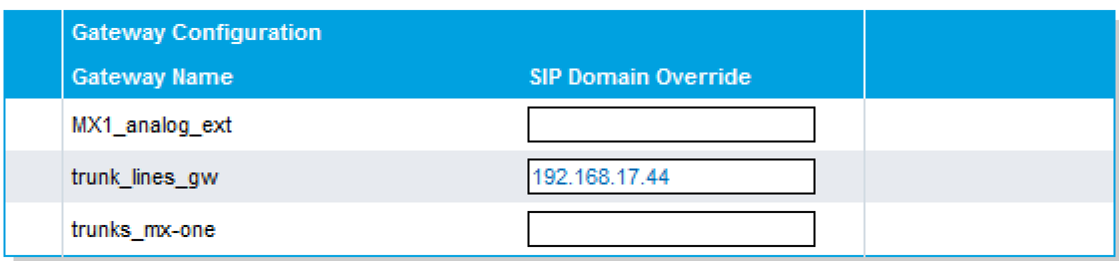
3. Click **Apply** or when done and restart service.

Misc

Figure 11.58: Misc

1. Enter the IP-address of MX-ONE in the **SIP Domain Override** field for **trunk_lines_gw**.

Figure 11.59: Gateway Configuration field



2. Click **Apply** when done and restart service.

Media

Codecs

Figure 11.60: Codecs

1. Change Codecs according to preference.

Figure 11.61: Changing Codecs

Codec	Voice	Data	Advanced
G.711 a-Law	Enable	Enable	
G.711 u-Law	Disable	Enable	
G.723	Disable		
G.726 16Kbps	Disable		
G.726 24Kbps	Disable		
G.726 32Kbps	Disable	Disable	
G.726 40Kbps	Disable	Disable	
G.729	Disable		
T.38		Enable	
Clear Mode	Disable	Disable	
Clear Channel	Disable	Disable	
X CCD	Disable	Disable	

2. Click **Apply** when done and restart service.

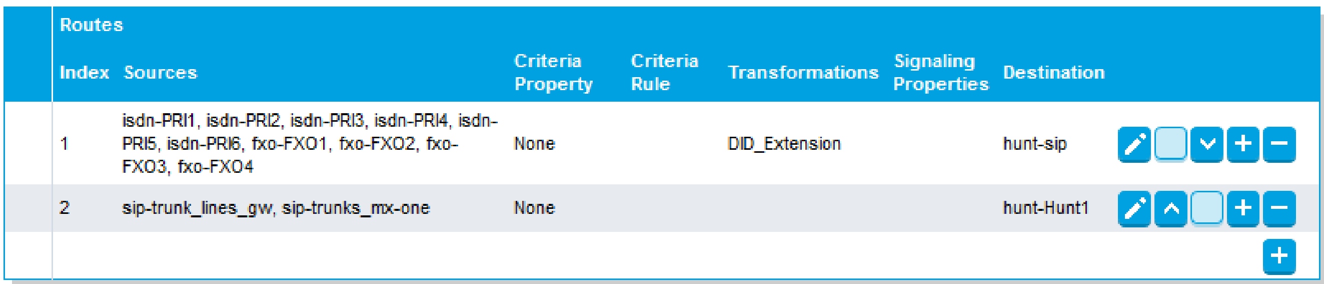
Call Router

Route Config

Figure 11.62: Route Config

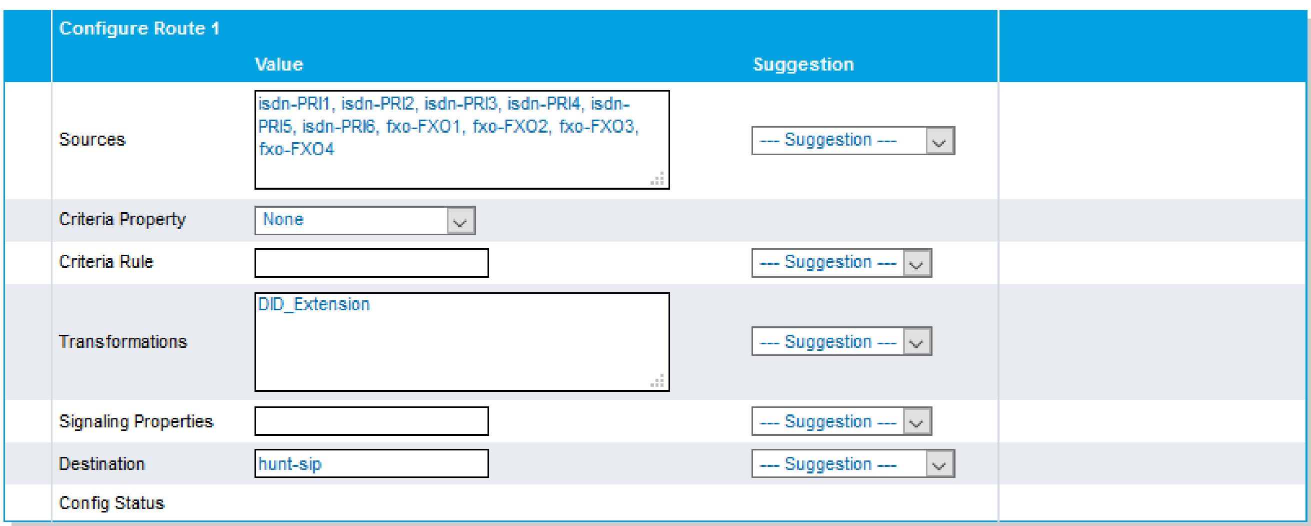
1. Click  for index 1. This is used if the received B-number contains a full number. That is, more digits than the pure DID numbers.

Figure 11.63: Routes screen



2. In the **Transformations** field add a name for a transformation rule.

Figure 11.64: Transformations field



3. Click **Save**.
4. Click  in the first Call Property Transformation and enter the same name as above.
5. Use **Called E164** for both **Criteria Based On** and **Transformation Applies To** fields.

Figure 11.65: Configure Transformation 1 Screen

Configure Transformation 1	Value
Name	DID_Extension
Criteria Based On	Called E164
Transformation Applies To	Called E164
Config Status	

6. Click **Save** or **Save and Insert Rule**.
7. Click in the second Call Property Transformation and enter the same name as above.
8. The 'Criteria Rule' in this case is 443 (111..)$ and the transformation rule is '\1. This means that if a B-number is received containing 44311104, then the 3 first digits (443) are removed before the call is sent to MX-ONE for further processing. (111..)$ means that the number can only be 5 digits starting with 111.

Figure 11.66: Configure Transformation Rule 1 screen

Configure Transformation Rule 1	Value	Suggestion
Type	Called E164 to Called E164	
Name	DID_Extension	--- Suggestion ---
Criteria Rule	443(111..$)	--- Suggestion ---
Transformation Rule	\1	--- Suggestion ---
Next Transformation		--- Suggestion ---
Config Status		

9. Click **Save** or **Save and Insert Rule**. Now, the 'Call Property Transformations' looks like this as shown below.

Figure 11.67: Transformations screen

Transformations

Index	Name	Criteria Based On	Transformation Applies To
1	DID_Extension	Called E164	Called E164

Transformation Rules

Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	DID_Extension	443(111..$)	\1	

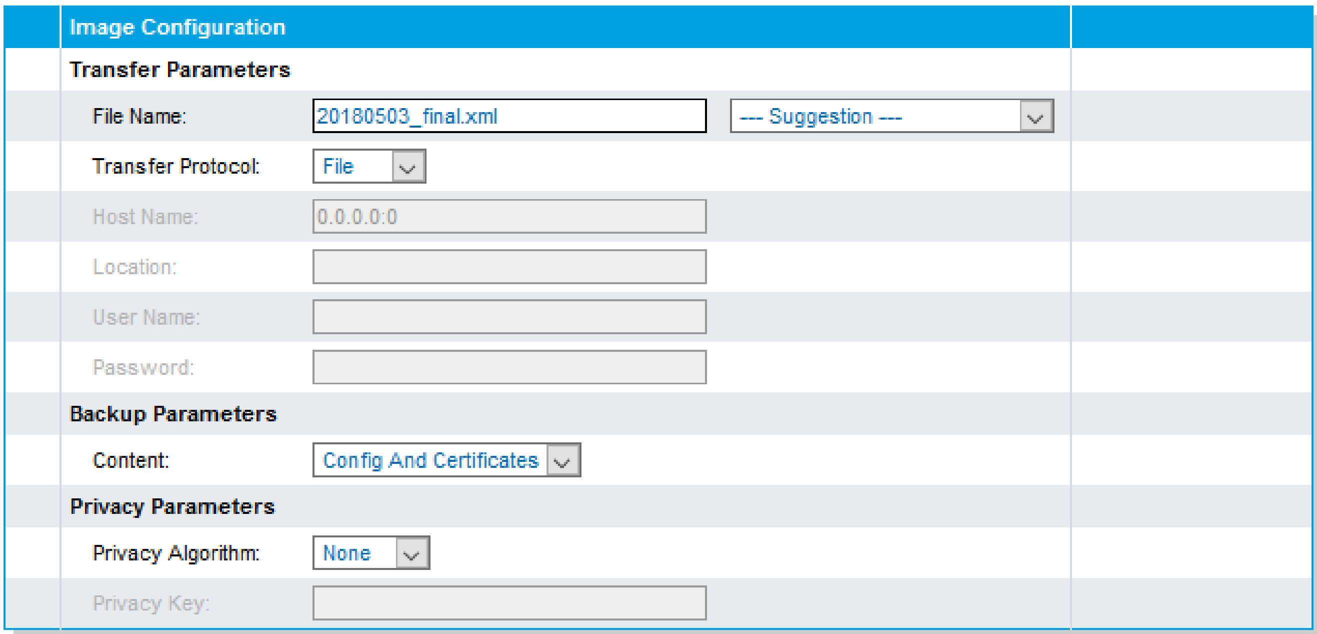
10. Click **Save** if the yellow indication on top of the page is ON.

Management

Backup/Restore

1. Click **Activate ....**

Figure 11.68: Image Configuration screen



2. Click **Apply and Backup Now**.

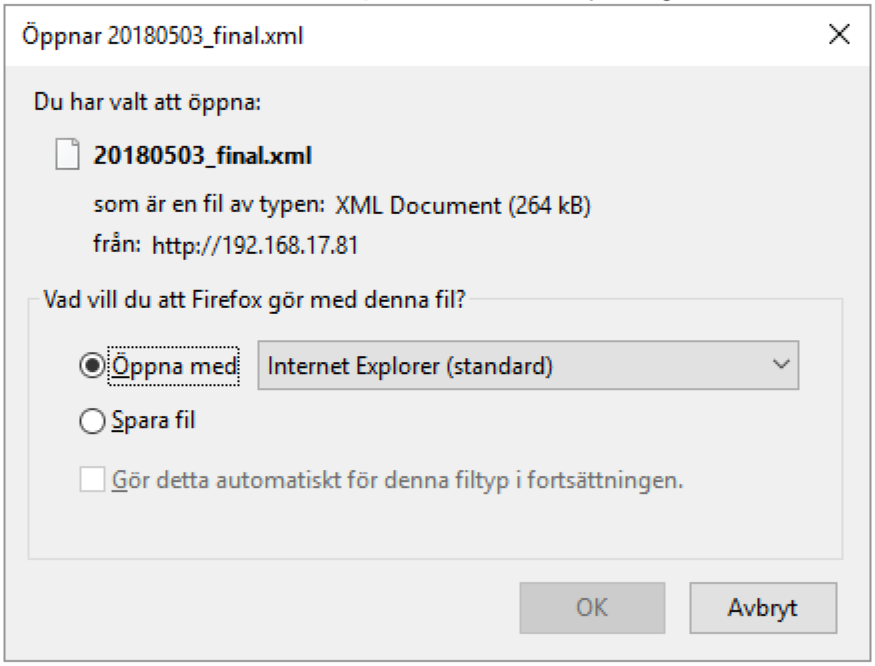
File

Figure 11.69: Internal files screen

Internal files		
Name	**Description**	**Size**
conf/20180503_final.xml	Automatically generated on 03/05/2018 15:50:11.	264 KB
conf/FXO_Country_Defaults.cfg	FXO Country Defaults	1 KB
conf/FXO_North-America_3km.cfg	FXO North-America 3km	1 KB
conf/PRI_China-DSS1.cfg	China DSS1	3 KB
conf/PRI_Default.cfg	PRI default configuration	3 KB
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB
conf/Survivability.cfg	Configures the unit to use the SipProxy service for basic use cases.	1 KB
sbc/rulesets/200_OK_to_SIP_OPTIONS.crs	Answer 200 OK to inbound SIP OPTIONS message	1 KB
sbc/rulesets/MX-One_build_RURI_survivability.crs	Builds the RURI when in survivability mode	6 KB
sbc/rulesets/MX-One_core_side.crs	Generic ruleset facing MX-One core	5 KB
sbc/rulesets/MX-One_local_reg_users_with_survivability.crs	local registered users ruleset for MX-One with basic local calling survivability	11 KB
sbc/rulesets/MX-One_local_users_failover_to_trunk.rrs	Failover route from local_users_ca to trunk_lines_ca	6 KB
sbc/rulesets/MX-One_outbound_survivability_prefix.crs	ANumber and BNumber prefix	2 KB
sbc/rulesets/MX-One_remove_prefix.crs	Removes prefix from RURI for outbound calls	1 KB
sbc/rulesets/MX-One_routes_with_basic_local_survivability_TCP.rrs	MX-One - Basic Routes with Survivability	23 KB
sbc/rulesets/MX-One_routes_with_basic_local_survivability_UDP.rrs	MX-One - Basic Routes with Survivability	21 KB
sbc/rulesets/MX-One_to_trunk_lines.rrs	Route from MX-One servers to trunk lines	5 KB
sbc/rulesets/MX-One_trunk_lines_to_local_users.rrs	Route from trunk_lines_ca to local_users_ca	3 KB
sbc/rulesets/MX-One_trunk_lines_to_reception_survivability.crs	Forwards trunk calls to reception number in survivability	2 KB
sbc/rulesets/rewrite_RURI_host.crs	Customize RURI host	1 KB
21 file(s)	Total: 366 KB / Available: 6 GB	

Find the previously made backup image

Figure 11.70: Backup image



Setting up MX-ONE for an EX Controller

The setting up of MX-ONE is not described in this document since it does not differ from an ordinary MX-ONE setup.

Setting up EX Controller

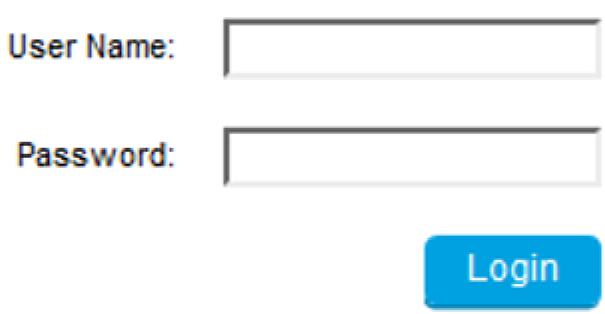
Logon

This section describes how to setup BO#1.

Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network).

NOTE: If DHCP is not running into the network then, plug in the network cable to the ETH2 port on EX Controller and use the default IP address of 192.168.0.10 to open the EX Controller Interface.

Figure 11.71: Logon screen



This section describes how to setup BO#1.

1. Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network).
   - User name/password: public /
   - User name/password: admin/administrator

2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.

3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

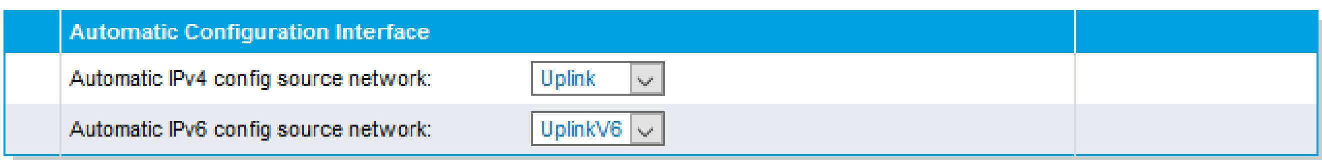
Network Settings

Host

1. Select **Network** > **Host** and keep the default configuration interface as mentioned below.

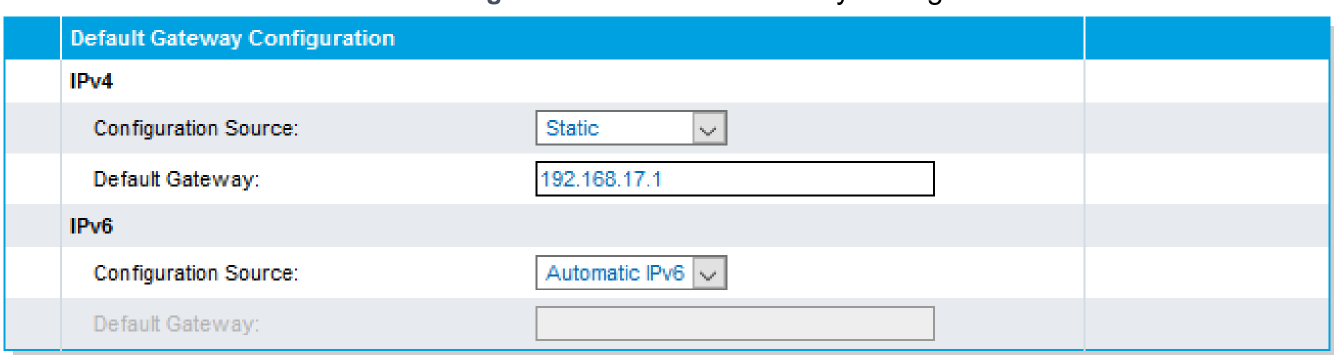
Figure 11.72: Host screen

Figure 11.73: Automatic Configuration Interface



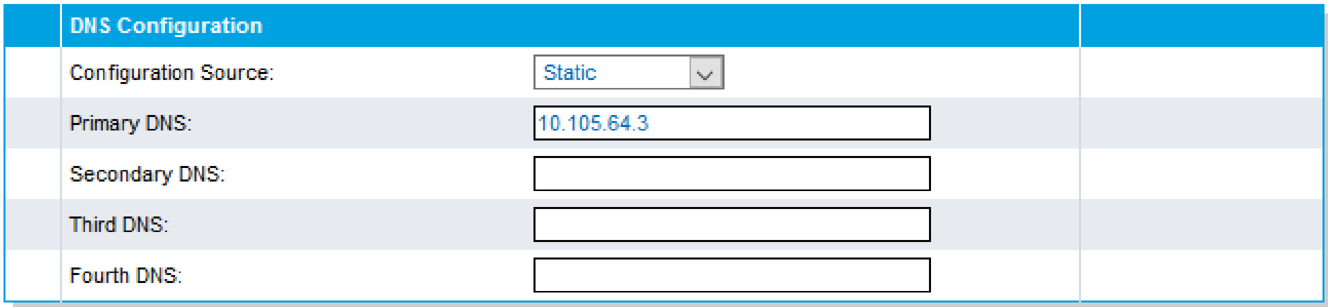
2. Change to Static IP-address and enter default Gateway (GW).

Figure 11.74: Default Gateway Configuration



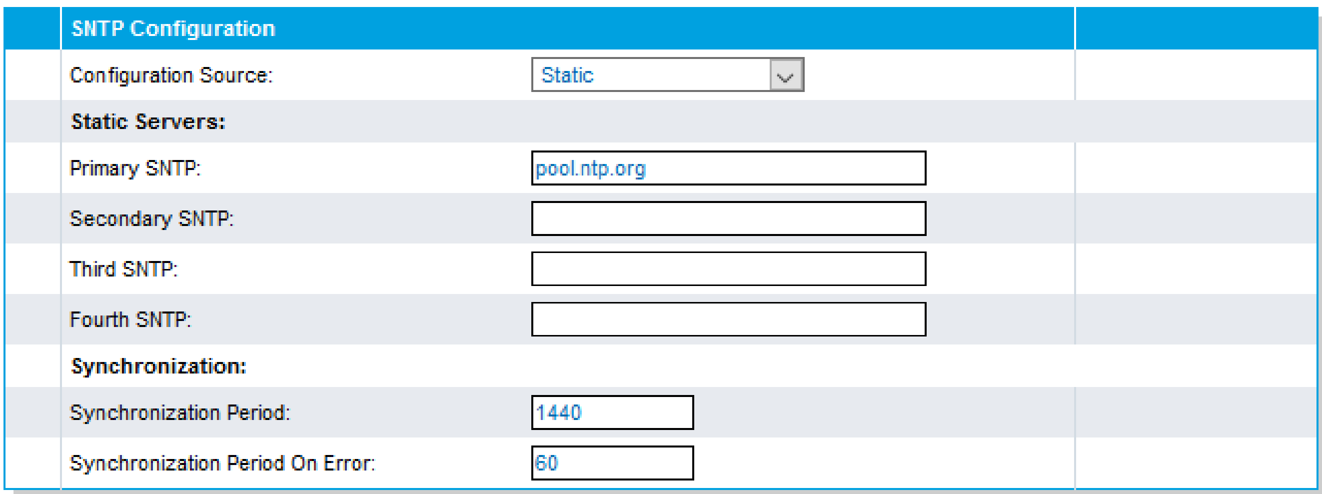
3. Change to static DNS server and enter IP-address or FQDN to DNS server.

Figure 11.75: DNS Configuration screen



4. Change to static SNTP server and enter time server data.

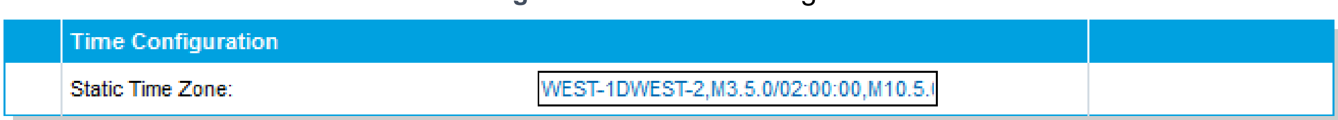
Figure 11.76: SNTP Configuration



5. Set the Static Time Zone. Valid options are:

– Pacific Time (Canada and US): PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
– Mountain Time (Canada and US): MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
– Central Time (Canada and US): CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
– Eastern Time (Canada and US): EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
– Atlantic Time (Canada): AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
– GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
– W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
– China Standard Time: CST-8
– Tokyo Standard Time: TST-9
– Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
– Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
– UTC (Coordinated Universal Time): UTC0

Figure 11.77: Time Configuration screen

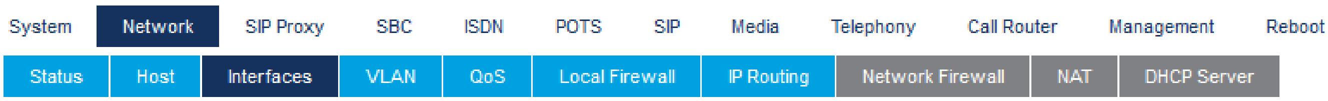


6. Leave all other items as it is and click **Apply** when finished.

Interfaces

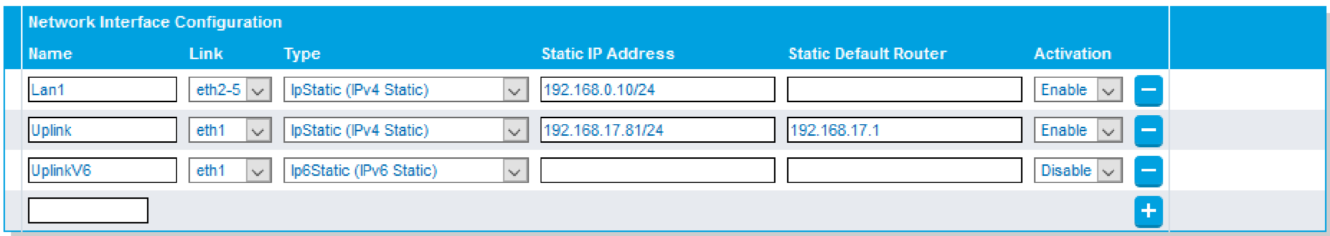
1. Go to **Network** > **Interface**.

Figure 11.78: Interfaces screen



2. Change **Uplink** to **IpStatic (IPv4 Static)** and enter the static IP-address and Static Default Gateway.

Figure 11.79: Network Interface Configuration



3. Leave all other items as it is and click **Apply** when ready.

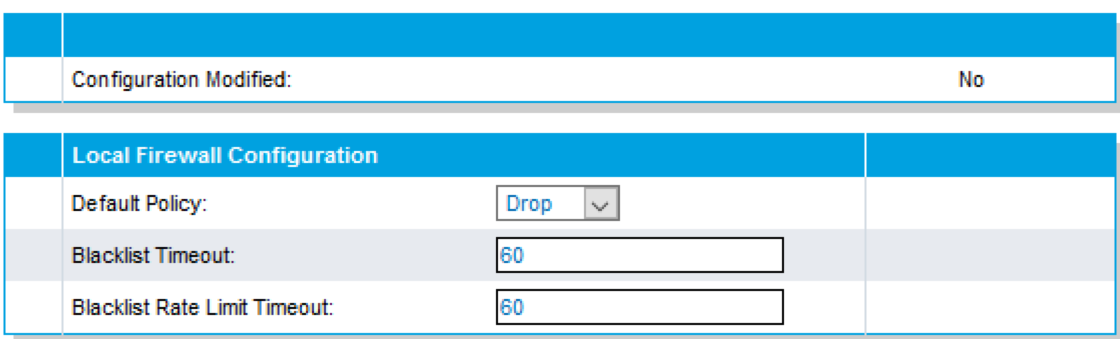
Local Firewalls

1. Go to **Network** > **Local Firewall**.

Figure 11.80: Local Firewall screen

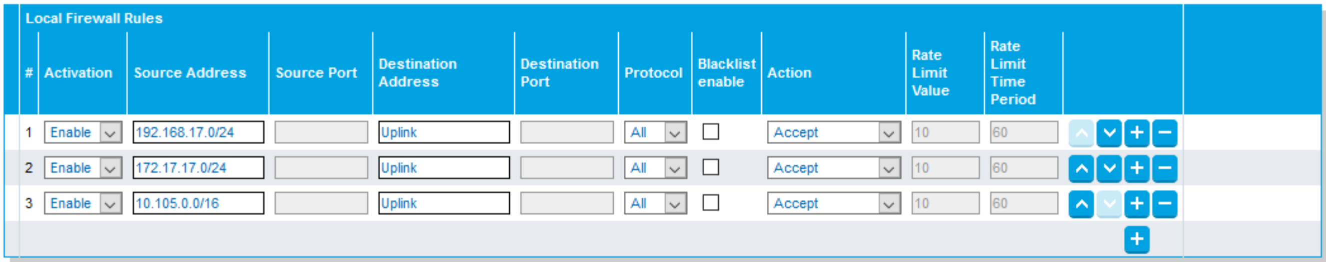
2. If local firewall security is needed, change default policy to **Drop**.

Figure 11.81: Local Firewall Configuration screen



3. Enter the networks for which traffic can enter from.

Figure 11.82: Local Firewall Rules screen



4. Click **Save** or **Save and Apply** when ready.

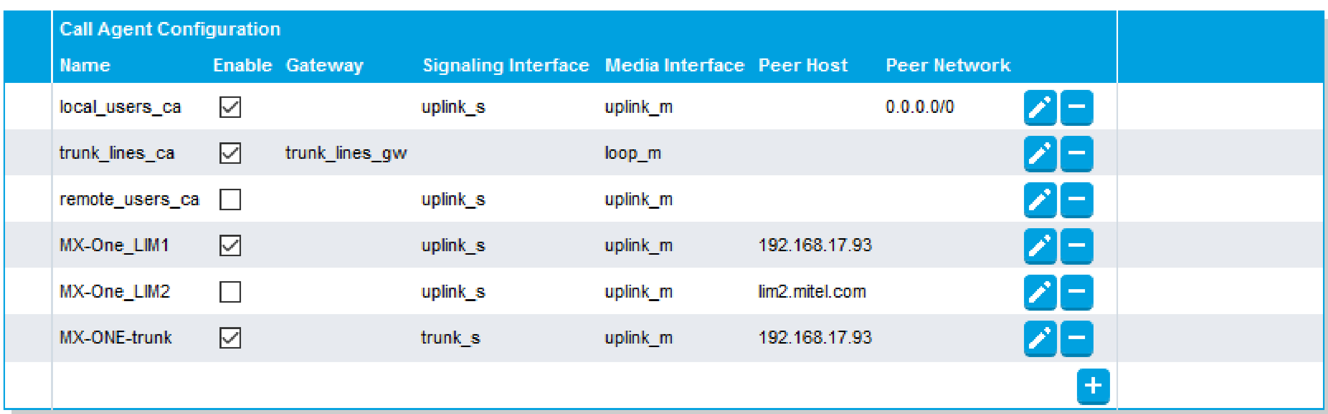
SBC

Configuration

1. Go to SBC > Configuration. The following Call Agents are present.

Figure 11.83: SBC Configuration screen

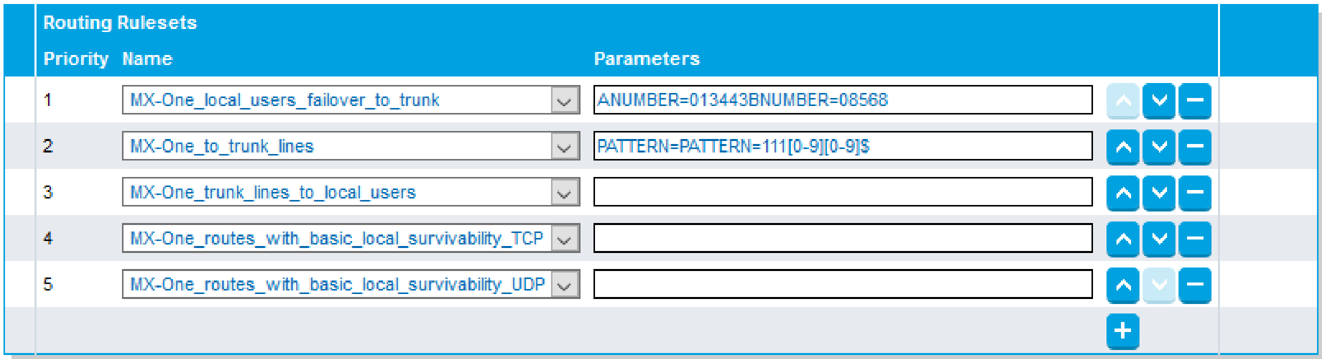
Figure 11.84: Call Agent Configuration screen



2. Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers when the GW is in survivable mode. That is, the call is routed to PSTN and thus needs to be prefixed.

3. Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 321[0-9][0-9]$ means that the allowed number range in this branch is 32100 – 32199.

Figure 11.85: Routing Rulesets screen



4. Configure each call agent (ca).
5. Click to enter specific data for each call agent.

Local_users_ca

- Enter the IP-address of MX-ONE to the DOMAIN variable.
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 321[0-9][0-9]$ means that the allowed number range in this branch is 32100 – 32199.
- Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers when the GW is in survivable mode. That is, the call is routed to PSTN and thus needs to be prefixed.

Figure 11.86: Configure Call Agent screen

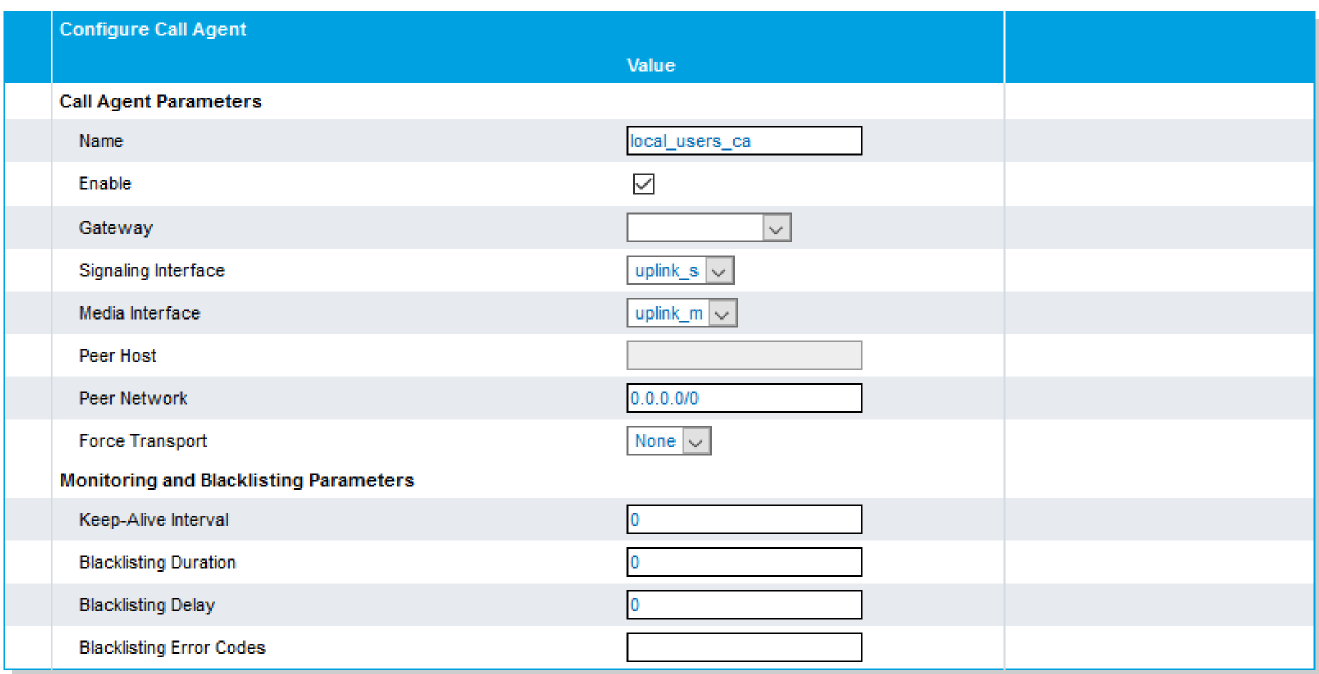


Figure 11.87: Call Agent Rulesets

Call Agent Rulesets

Priority	Name	Parameters
1	MX-One_build_RURI_survivability	PATTERN=321[0-9][0-9]$ DOMAIN=192.168.17.94
2	MX-One_Appearance_Prefix	APP_PRFX=SCA-
3	MX-One_Appearance_Prefix	APP_PRFX=EDN-
4	MX-One_Remove_Outbound_Appearance	PATTERN=321[0-9][0-9]$
5	MX-One_outbound_A_Number_prefix	PATTERN=321[0-9][0-9]$ A_PRFX=anumber_prefix PSTN_PREF
6	MX-One_outbound_B_Number_prefix	BNUMBER=67[0-9][0-9][0-9]$ B_PRFX=08568
7	MX-One_outbound_B_Number_prefix	BNUMBER=111[0-9][0-9]$ B_PRFX=013443
8	MX-One_outbound_B_Number_prefix	BNUMBER=221[0-9][0-9]$ B_PRFX= 031325
9	MX-One_outbound_B_Number_Override	BNUMBER=440[0-9][0-9]$ BOVERRIDE=0856867000
10	MX-One_local_reg_users_with_survivability	EXT_DIGIT_LENGTH=5

Ruleset MX-One_build_RURI survivability (ACTIVE ONLY IN SURVIVAL MODE)

PATTERN=111[0-9][0-9]$

The pattern for the internal range of numbers, in this example the internal range would be 11100 – 11199

Calls to this number range stay always local (would not send to the PSTN in survival mode)

DOMAIN=192.168.17.94

The IP-address of the MX-ONE instance running on the VM, in this case 192.168.17.94

Ruleset: MX_One_Appearance_Prefix (ACTIVE ONLY IN SURVIVAL MODE)

NEW: APP_PREFIX=SCA-

This is the prefix for the usernames connected with shared appearance. In this example, you have two: “SCA-“ and “EDN-“

Ruleset: MX-One_Remove_Outbound_Appearance (ACTIVE ONLY IN SURVIVAL MODE)

PATTERN=321[0-9][0-9]$

This rule removes any prefix used for Shared Call Appearance. The pattern for the internal range of numbers, in this example the internal range would be 32100 – 32199

Ruleset: MX-One_outbound_A_Number_prefix (ACTIVE ONLY IN SURVIVAL MODE)

PATTERN=321[0-9][0-9]

This defines the local numbers.

A_PRFX=040598

This is the prefix for the local numbers used on outgoing calls to the PSTN (in this example, received a number block 013443xxxxx from the PSTN provider and add the prefix on outgoing calls, so that the calling party number sent to the PSTN is correct)

PSTN_PREFIX=00

Dial this prefix to break out to the PSTN. Here, you need to configure the “00” (not to be mixed up with the “00” for international calls!)

Ruleset: MX-One_outbound_B_Number_prefix (ACTIVE ONLY IN SURVIVAL MODE)

This ruleset applies to calls to numbers defined in BNUMBER and will add B_PRFX to the called party number.

BNUMBER=67[0-9][0-9]$

Applies to calls to the specific range of extensions,

B_PRFX=08568

This is the prefix for the Called Party Number. In this case, it was build like: National Prefix (08) + Main part of the HQ's local number: (568), in case somebody dials an extension in the HQ.

Ruleset: MX-One_outbound_B_Number_Override (ACTIVE ONLY IN SURVIVAL MODE)

This ruleset applies to calls to numbers defined in BNUMBER and will use the BOVERRIDE as Called Party Number.

BNUMBER=440[0-9][0-9]$

Applies to calls to the specific range

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE, in this example they will be sent to 0856867000

Ruleset: MX-One_local_reg_users_with_survivability

(Builds the registration cache for survivability purpose)

EXT_DIGIT_LENGTH=5

The length of the internal numbers, in this case set to "5", for numbers like "00001 – 99999"

1. Click **Save** when done.

Trunk_Lines_ca

- Enter the IP-address of MX-ONE to the DOMAIN variable (in two places).
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 321[0-9][0-9]$ means that the allowed number range in this branch is 32100 – 32199.
- Insert a main extension number in MAIN_EXT parameter, this is could be the local answering position when dialling a vacant number, and so on.
- Enter the PSTN_PREFIX and STRIPNDIGTS, this is used to remove the public access code when dialling PSTN calls in survivable mode.

Figure 11.88: Configure Call Agent screen

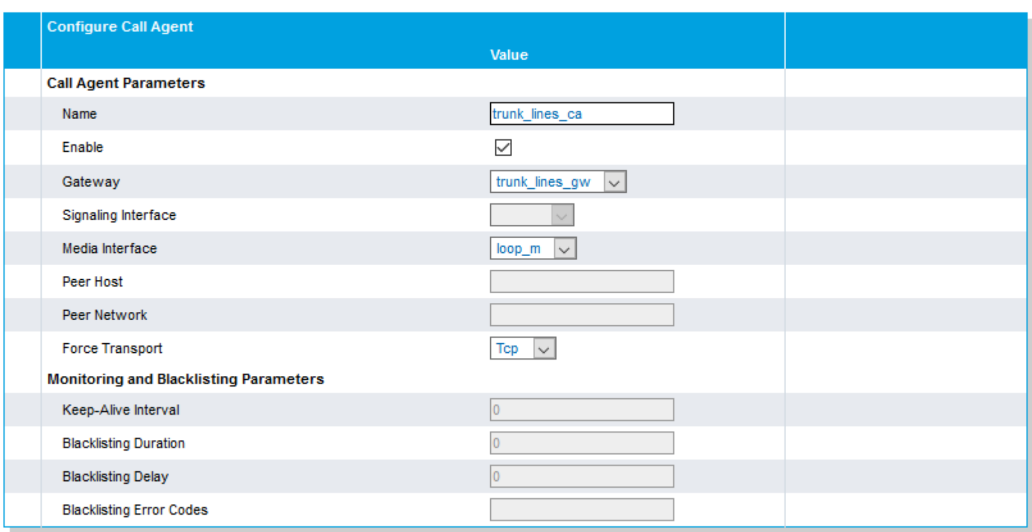
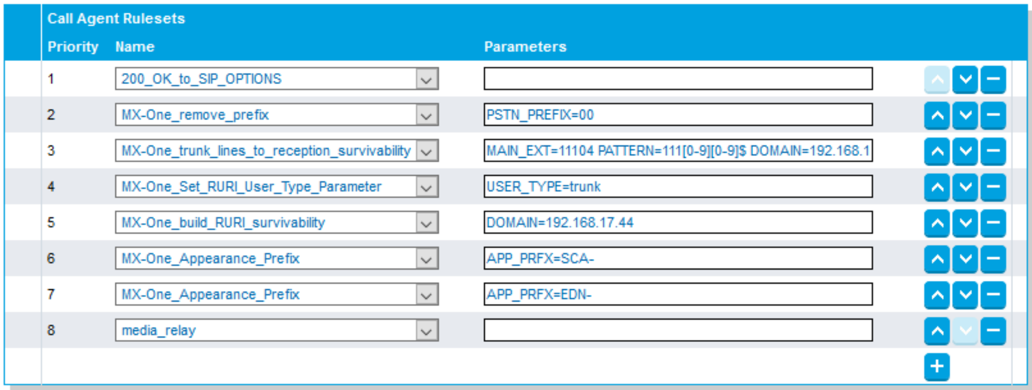


Figure 11.89: Call Agent Rulesets



Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This is the prefix used to dial out to the PSTN

Ruleset: MX-One_trunk_lines_to_reception_survivability

An incoming call in survival mode will be sent to MAIN_EXT destination if not reachable

MAIN_EXT=11104

This will receive the incoming call in case the original destination is not reachable (not defined or not registered)

PATTERN=321[0-9][0-9]$

The pattern for the internal range of numbers, in this example the internal range would be 32100 – 32199

DOMAIN=192.168.17.94

The IP of the headquarter (the main PBX), in this case 192.168.17.94

Ruleset: MX-One_Set_RURI_User_Type_Parameter

Set RURI User Type Parameter

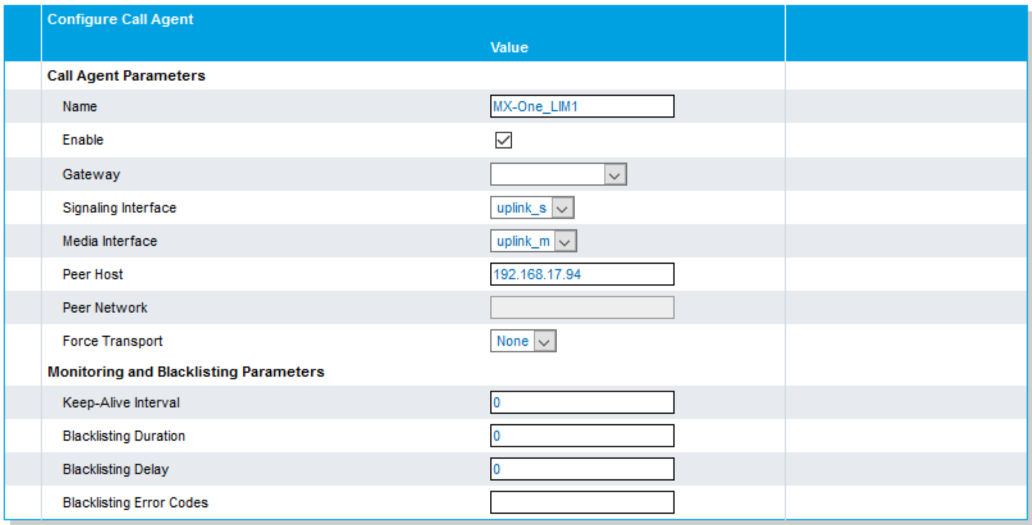
USER_TYPE=trunk

1. Click **Save** when done.

MX-ONE_Lim1

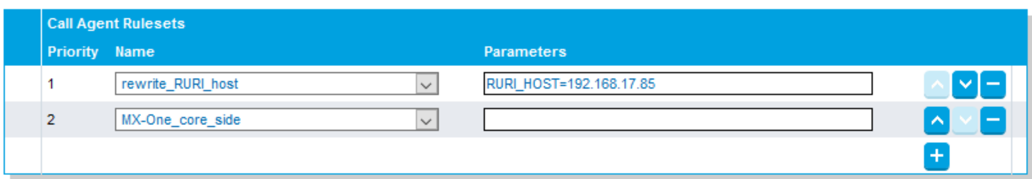
1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 11.90: Peer Host field



2. Enter the IP-address of the GW in the **RURI_HOST** parameter.

Figure 11.91: RURI_HOST parameter



Ruleset: rewrite_RURI_host

Customize RURI host

RURI_HOST= 192.168.17.85. This is the local IP address.

1. Click **Save** when ready.

MX-ONE_TRUNK

1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 11.92: Call Agent Parameters

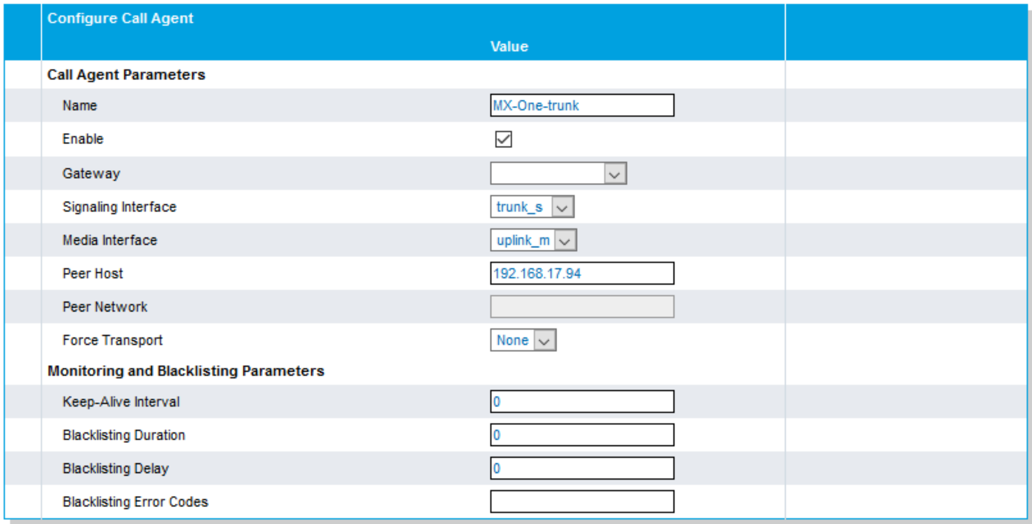
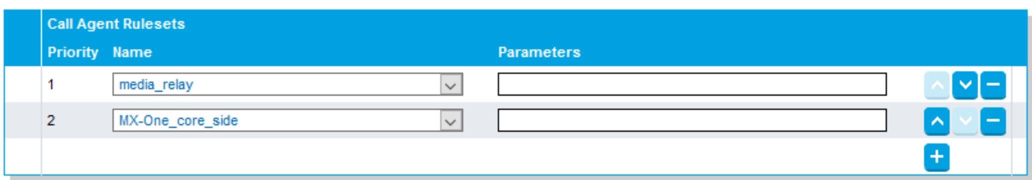


Figure 11.93: Call Agent Rulesets



2. When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.

3. Click **Save** when ready.

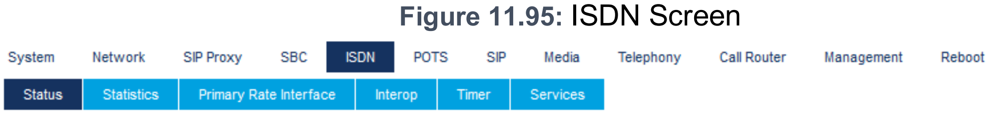
Figure 11.94: Configuration Modified screen

4. If the indication is not removed there are some error in the configuration.

5. Double check changes described above and correct them.

ISDN

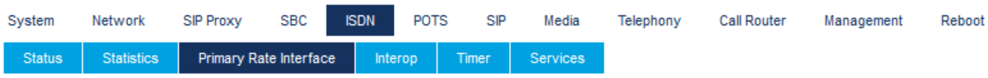
Figure 11.95: ISDN Screen



If ISDN trunks are used the first action to do is to click **Start Sensing**. The system automatically detects certain parameters, for example, number of channels.

Primary Rate Interface

Figure 11.96: Primary Rate Interface screen



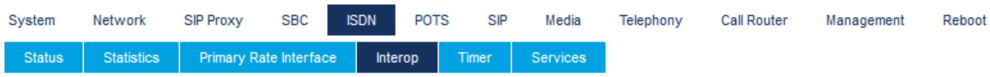
1. When sensing is done for several markets, specific parameters can be changed.

Interface Configuration	
Line Type: [Configure]	E1
Endpoint Type:	TE
Clock Mode:	Slave
Port Pinout:	Auto
Monitor Link State:	Enable
Line Coding:	HDB3
Line Framing:	CRC4
Signaling Protocol:	DSS1
Network Location:	User
Preferred Encoding Scheme:	G.711 a-Law
Fallback Encoding Scheme:	G.711 u-Law
Channel Range:	1-30
Channels Reserved for Incoming Calls:	
Channels Reserved for Outgoing Calls:	
Channel Allocation Strategy:	Ascending
Maximum Active Calls:	30
Signal Information Element:	Disable
Inband Tone Generation:	Enable
Inband DTMF Dialing:	Enable
Overlap Dialing:	Disable
Calling Name Max Length:	34
Exclusive B-Channel Selection:	Disable
Sending Complete:	Enable
Send Restart On Startup:	Enable
Link Establishment:	Permanent
Accepted Status Causes:	
Accepted Progress Causes:	1-127
Send Isdn Progress:	Send All
Send Progress Indicator IE:	Send All
Default TON for Calling Party Number IE:	National
Default NPI for Calling Party Number IE:	Isdn Telephony
Default PI for Calling Party Number IE:	Presentation Allowed
Default SI for Calling Party Number IE:	Context Dependent
Default TON for Called Party Number IE:	National
Default NPI for Called Party Number IE:	Isdn Telephony
Notification User Suspended:	Ignore

1. Click Apply and restart requested service when done.

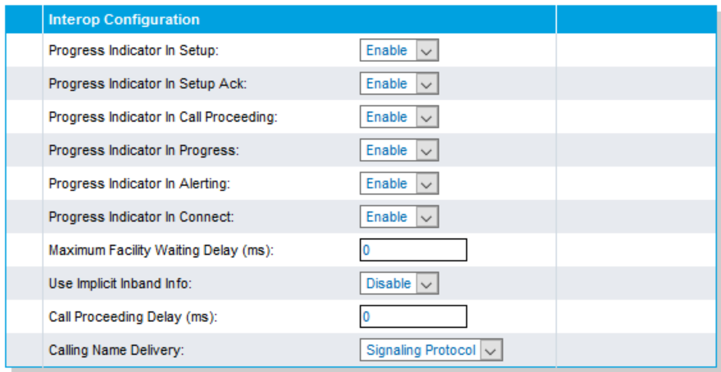
Interop

Figure 11.97: Interop screen



1. You can change other parameters dependent on market.

Figure 11.98: Interop Configuration screen

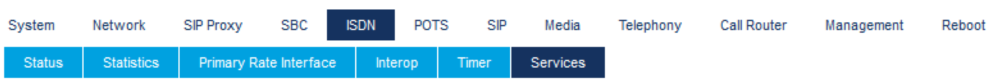


Interop Configuration	
Progress Indicator In Setup:	Enable
Progress Indicator In Setup Ack:	Enable
Progress Indicator In Call Proceeding:	Enable
Progress Indicator In Progress:	Enable
Progress Indicator In Alerting:	Enable
Progress Indicator In Connect:	Enable
Maximum Facility Waiting Delay (ms):	0
Use Implicit Inband Info:	Disable
Call Proceeding Delay (ms):	0
Calling Name Delivery:	Signaling Protocol

2. Click **Apply** and restart requested service when done.

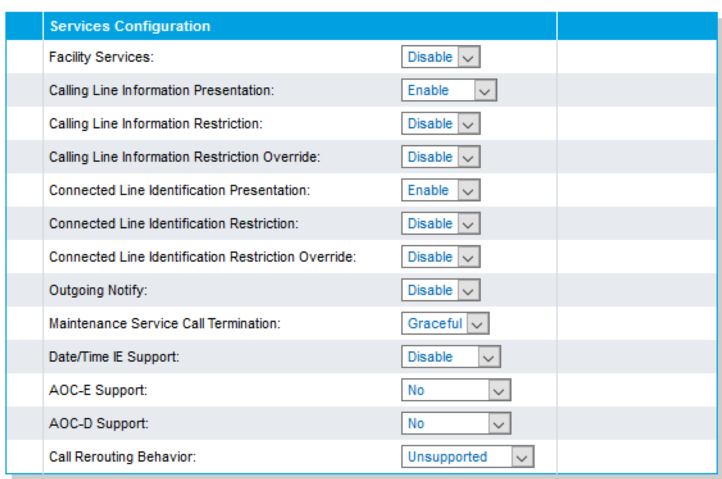
Services

Figure 11.99: ISDN Services screen



1. Change other parameters dependent on market.

Figure 11.100: Services Configuration screen



Services Configuration	
Facility Services:	Disable
Calling Line Information Presentation:	Enable
Calling Line Information Restriction:	Disable
Calling Line Information Restriction Override:	Disable
Connected Line Identification Presentation:	Enable
Connected Line Identification Restriction:	Disable
Connected Line Identification Restriction Override:	Disable
Outgoing Notify:	Disable
Maintenance Service Call Termination:	Graceful
Date/Time IE Support:	Disable
AOC-E Support:	No
AOC-D Support:	No
Call Rerouting Behavior:	Unsupported

2. Click **Apply** and restart requested service when done.

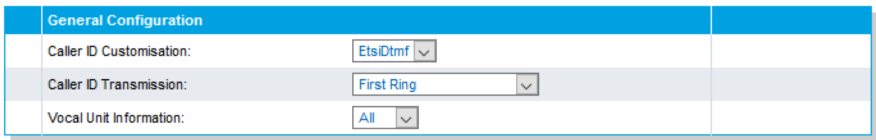
POTS

Config

Figure 11.101: Config screen

1. Set market specific data for Caller Id handling.

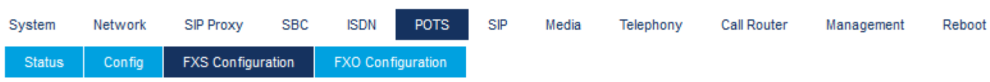
Figure 11.102: General Configuration screen



2. Click **Apply** when done and restart service.

FXS Configuration

Figure 11.103: POTS FXS Configuration screen



1. Set analog phone specific data according to market.

Figure 11.104: FXS Configuration screen

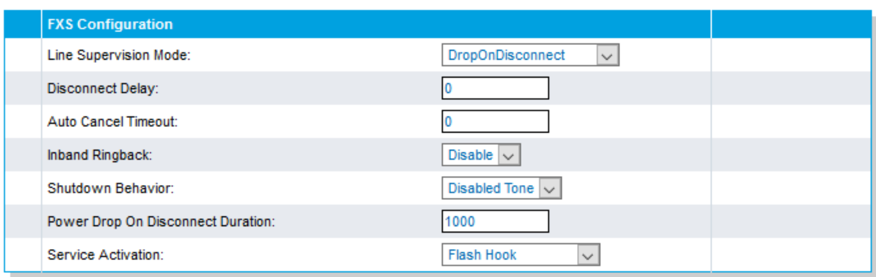
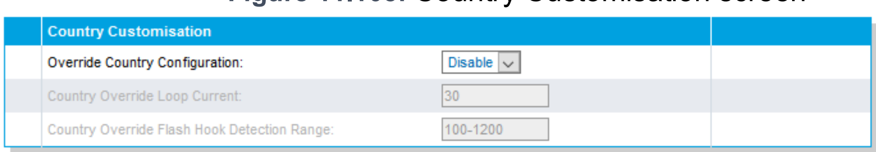


Figure 11.105: Country Customisation screen



2. Click **Apply** when done and restart service.

SIP

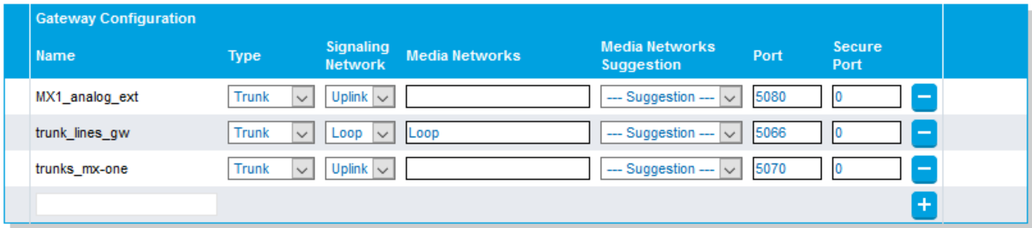
Gateways

Following gateways and port numbers are pre-defined.

Figure 11.106: Gateways screen

NOTE: A SIP route must be defined in MX-ONE to handle traffic to and from the 'trunks_MX-ONE' gateway.

Figure 11.107: Gateway Configuration screen



Gateway Configuration

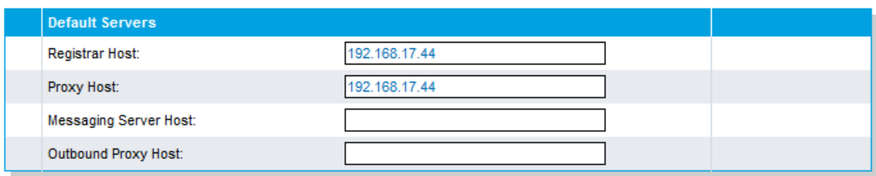
Name	Type	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port
MX1_analog_ext	Trunk	Uplink		--- Suggestion ---	5080	0
trunk_lines_gw	Trunk	Loop	Loop	--- Suggestion ---	5066	0
trunks_mx-one	Trunk	Uplink		--- Suggestion ---	5070	0

Servers

Figure 11.108: Servers screen

1. Enter IP-address to MX-ONE in both **Registrar Host** and **Proxy Host** fields.

Figure 11.109: Default Servers screen

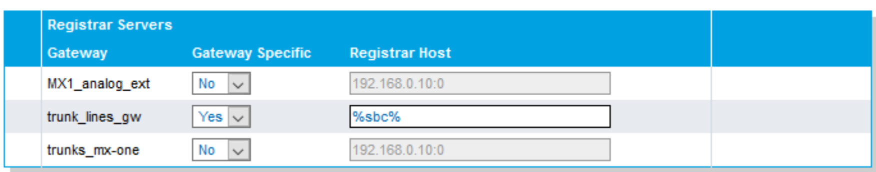


Default Servers

Registrar Host:	192.168.17.44
Proxy Host:	192.168.17.44
Messaging Server Host:	
Outbound Proxy Host:	

2. Change **trunk_lines_gw** to **Yes** in the drop-down list for **Gateway Specific**.

Figure 11.110: Registrar Servers screen

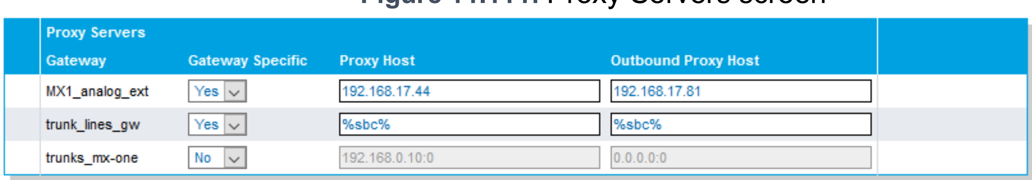


Registrar Servers

Gateway	Gateway Specific	Registrar Host
MX1_analog_ext	No	192.168.0.10:0
trunk_lines_gw	Yes	%sbc%
trunks_mx-one	No	192.168.0.10:0

3. Enter IP-address of MX-ONE in the **Proxy Host** field.
4. Enter IP-address of the gateway in the **Outbound Proxy** Host.

Figure 11.111: Proxy Servers screen



Proxy Servers

Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
MX1_analog_ext	Yes	192.168.17.44	192.168.17.81
trunk_lines_gw	Yes	%sbc%	%sbc%
trunks_mx-one	No	192.168.0.10:0	0.0.0.0:0

5. Enter the IP-address of the gateway as **Alternate Destination** for **MX1_analog_ext**.
6. Enter the IP-address of MX-ONE as **Alternate Destination** for **trunks_mx-one**.

Figure 11.112: Keep Alive Destination screen

Keep Alive Destination	
Gateway	**Alternate Destination**
MX1_analog_ext	192.168.17.85
trunk_lines_gw	127.0.0.1
trunks_mx-one	192.168.17.94

7. Click **Apply** when done and restart service.

Registrations

Figure 11.113: Registrations screen

1. Enter the extension numbers for the analog extensions.

Figure 11.114: Endpoints Registration screen

Endpoints Registration					
Endpoint	**User Name**	**Friendly Name**	**Register**	**Messaging**	**Gateway Name**
Slot1/E1T1			Disable	Disable	trunks_mx-one
Slot2/E1T1			Disable	Disable	trunks_mx-one
Slot3/FXS1	32104		Enable	Disable	MX1_analog_ext
Slot3/FXS2	32105		Enable	Disable	MX1_analog_ext
Slot3/FXS3	32106		Enable	Disable	MX1_analog_ext
Slot3/FXS4	32107		Disable	Disable	MX1_analog_ext
Slot4/E1T1			Disable	Disable	trunks_mx-one
Slot5/E1T1			Disable	Disable	trunks_mx-one

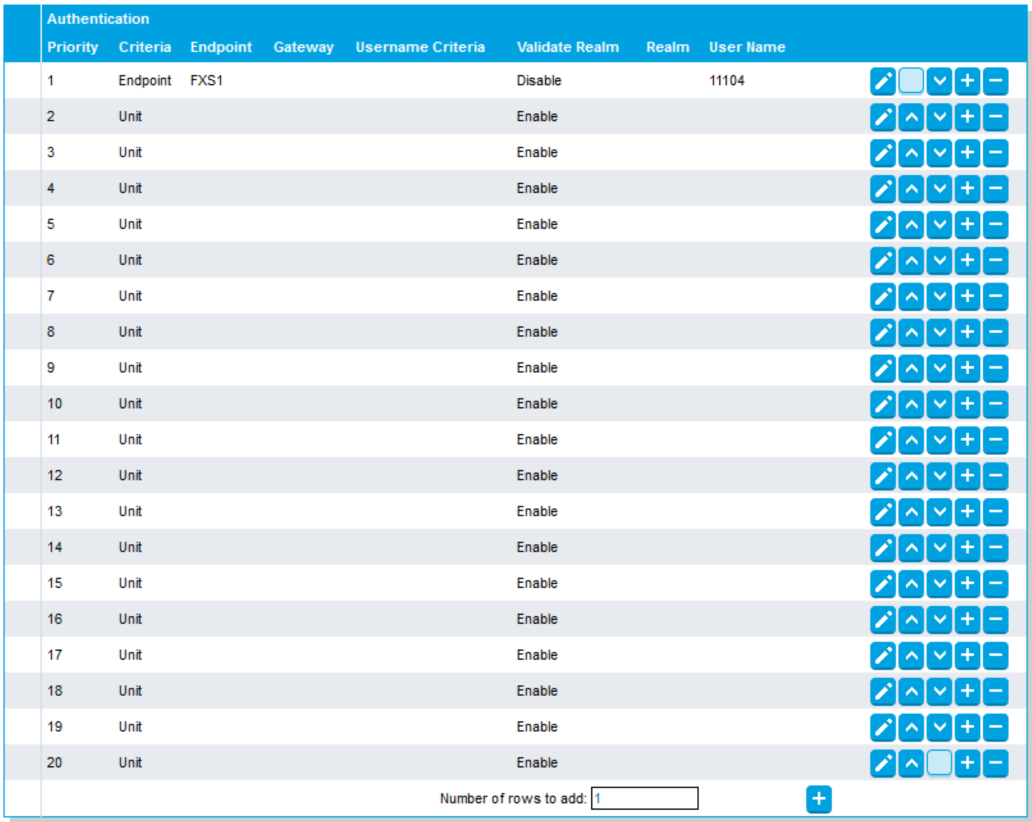
2. Click **Apply** or **Apply and Refresh** when done.

Authentication

Figure 11.115: SIP Authentication screen

1. If password is required, click for any item.

Figure 11.116: Authentication screen



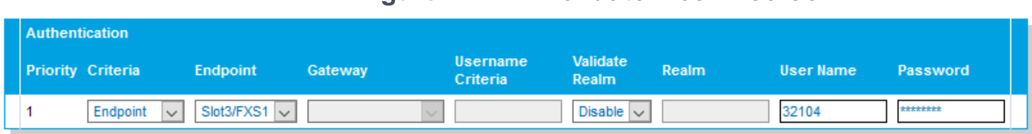
Authentication

Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name
1	Endpoint	FXS1			Disable		11104
2	Unit				Enable		
3	Unit				Enable		
4	Unit				Enable		
5	Unit				Enable		
6	Unit				Enable		
7	Unit				Enable		
8	Unit				Enable		
9	Unit				Enable		
10	Unit				Enable		
11	Unit				Enable		
12	Unit				Enable		
13	Unit				Enable		
14	Unit				Enable		
15	Unit				Enable		
16	Unit				Enable		
17	Unit				Enable		
18	Unit				Enable		
19	Unit				Enable		
20	Unit				Enable		

Number of rows to add: 1

2. Indicate for which Endpoint and Criteria changes are applicable.
3. Enter the Auth Code, in the **Password** field.
4. Disable Validate Realm.

Figure 11.117: Validate Realm screen



Authentication

Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Endpoint	Slot3/FXS1			Disable		32104	********

5. Click **Apply** or **Apply and Refresh Registration** when done and restart service. The result after 'Registration' and 'Authentication' should be like as follows.

Figure 11.118: Endpoints Registration screen

Endpoints Registration Status				
Endpoint	**User Name**	**Gateway Name**	**Registrar**	**Status**
Slot3/FXS1	32104	MX1_analog_ext	192.168.17.93:0	Registered
Slot3/FXS2	32105	MX1_analog_ext	192.168.17.93:0	Registered
Slot3/FXS3	32106	MX1_analog_ext	192.168.17.93:0	Registered

Transport

Figure 11.119: Transport screen

1. Enable UDP if required.

Figure 11.120: Protocol Configuration screen

Protocol Configuration					
UDP	**UDP QValue**	**TCP**	**TCP QValue**	**TLS**	**TLS QValue**
Enable		Enable		Disable	

2. Click **Apply** when done and restart service.

Misc

Figure 11.121: Misc screen

1. Enter the IP-address of MX-ONE in the **SIP Domain Override** filed for **trunk_lines_gw**.

Figure 11.122: Gateway Configuration screen

Gateway Configuration	
Gateway Name	**SIP Domain Override**
MX1_analog_ext	
trunk_lines_gw	192.168.17.94
trunks_mx-one	

2. Click **Apply** when done and restart service.

Media

Codecs

Figure 11.123: Codecs screen

1. Change Codecs according to preference.

Figure 11.124: Changing Codecs

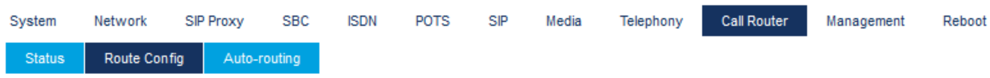
Codec	Voice	Data	Advanced
G.711 a-Law	Enable	Enable	
G.711 u-Law	Disable	Enable	
G.723	Disable		
G.726 16Kbps	Disable		
G.726 24Kbps	Disable		
G.726 32Kbps	Disable	Disable	
G.726 40Kbps	Disable	Disable	
G.729	Disable		
T.38		Enable	
Clear Mode	Disable	Disable	
Clear Channel	Disable	Disable	
X CCD	Disable	Disable	

2. Click **Apply** when done and restart service.

Call Router

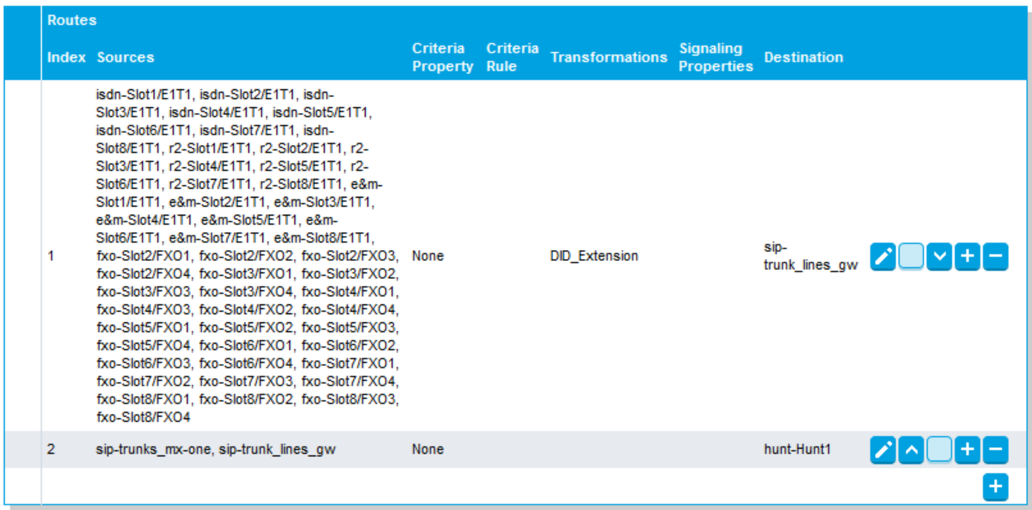
Route Config

Figure 11.125: Route Config screen



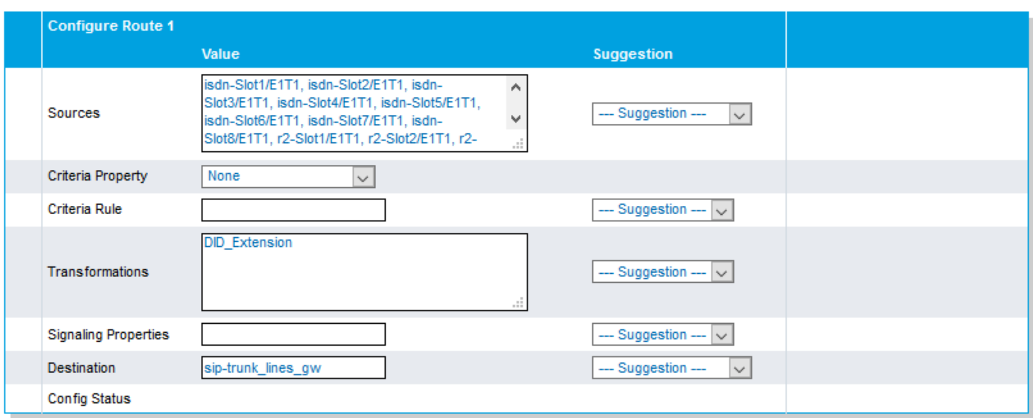
1. Click for index 1. This is used if the received B-number contains a full number. That is, more digits than the pure DID numbers.

Figure 11.126: Routes screen



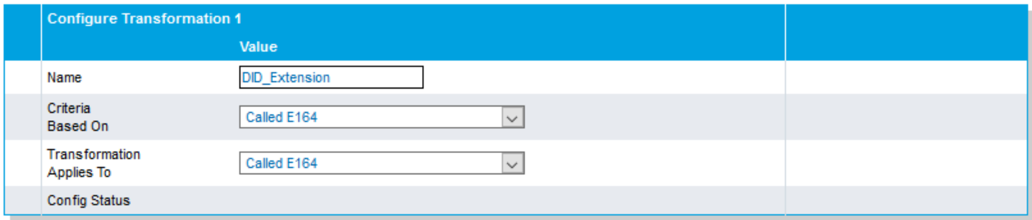
2. In the Transformations field add a name for a transformation rule.

Figure 11.127: Configure Route screen



3. Click **Save**.
4. Click in the first Call Property Transformation and enter the same name as above.
5. Use Called E164 for both **Criteria Based On** and **Transformation Applies To** fields.

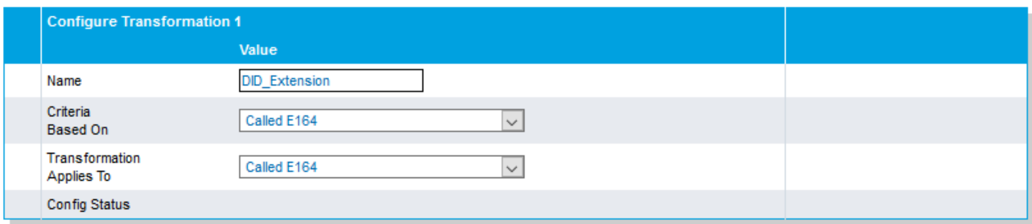
Figure 11.128: Configure Transformation screen



6. Click **Save** or **Save and Insert Rule**.
7. Click in the second Call Property Transformation and enter the same name as above.

8. Use Called E.164 for both **Criteria Based On** and **Transformation Applies To** fields.

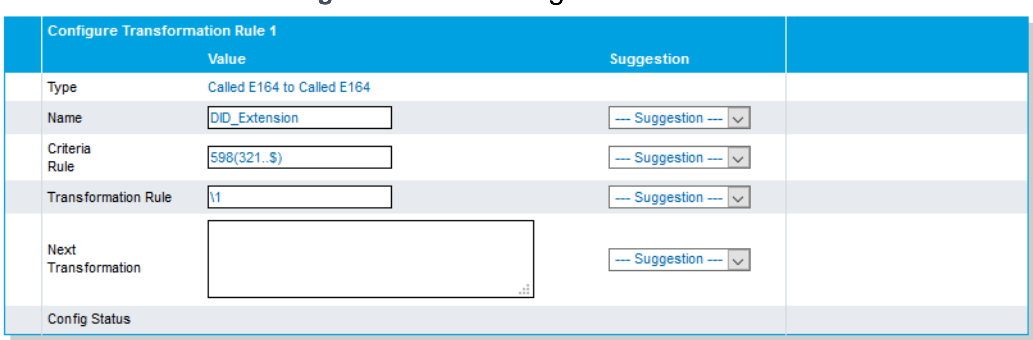
Figure 11.129: Configure Transformation screen 1



9. Click **Save** or **Save and Insert Rule**.
10. Click in the second Call Property Transformation, and enter the same name as above.

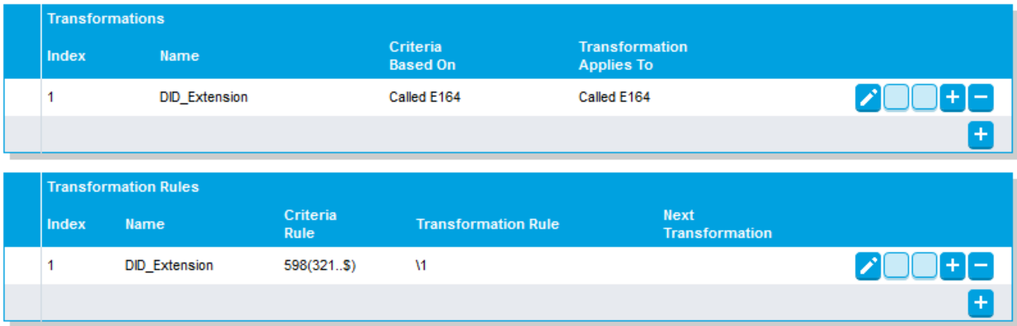
11. The Criteria Rule in this case is 443(111..)$ and the transformation rule is '\1.
12. This means that if a B-number is received containing 44311104, then the 3 first digits (443) are removed before the call is sent to MX-ONE for further processing. (111..)$ means that the number can only be 5 digits starting with 111.

Figure 11.130: Configure Transformation Rule 1



13. Click **Save** or **Save and Insert Rule**. Now, the 'Call Property Transformations' looks like this as shown below.

Figure 11.131: Transformations screen



14. Click **Save** if the yellow indication on top of the page is ON.

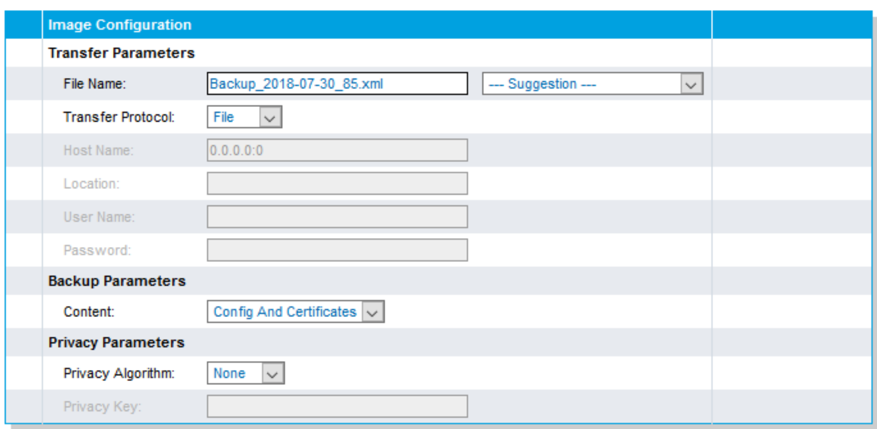
Management

Figure 11.132: Management screen

Backup/Restore

1. Click the **Activate unsecure script transfers through web browser** link.

Figure 11.133: Image Configuration screen



2. Click **Apply and Backup Now**.

File

Figure 11.134: File screen

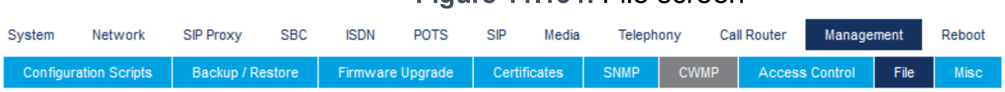
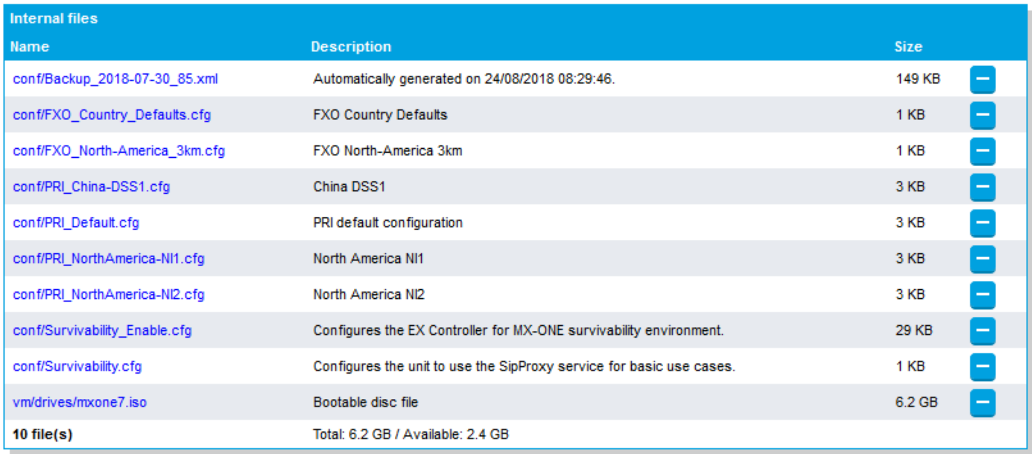
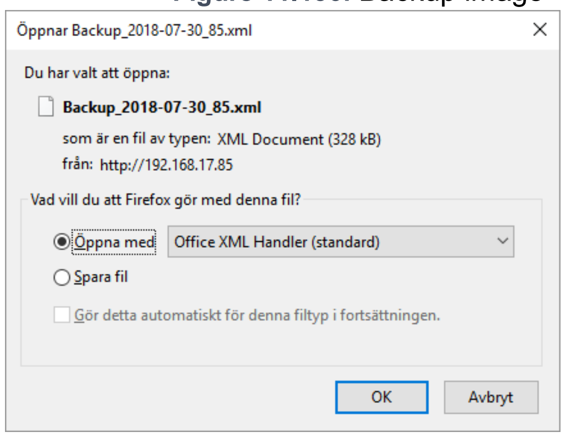


Figure 11.135: Internal files screen



1. Find the previously made backup image.

Figure 11.136: Backup image



2. Download and store on a secure place.

Configure TLS on an EX/GX Controller

This section describes how to configure TLS on an EX/GX controller with a typical scenario for a branch office with survivability and local presence. TLS ensures secure communication between the MX-ONE system and the EX and GX controller.

Prerequisites

Before you configure the TLS on the controller, ensure that the following requirements are met:

- The EX/GX controller setup is complete without TLS before you configure TLS on the controller. See the previous chapters in this document for the setup information.
- The EX/GX controller setup is fully loaded and the virtual machine on which MX-ONE has been setup is switched on.
- The FXS extensions are registered. You can view the registration status in the path **SIP > Registrations**.

- The FXS extensions need to be in the SBC registration cache. You can view in the path **SBC > Registration**.
- The TLS certificate authority is generated and is available in the path `/etc/opt/eri_sn/certs/root` with:
  - Certificate authority file: `/etc/opt/eri_sn/certs/root/CA.pem`
  - Private key: `/etc/opt/eri_sn/certs/root/private_key.pem`

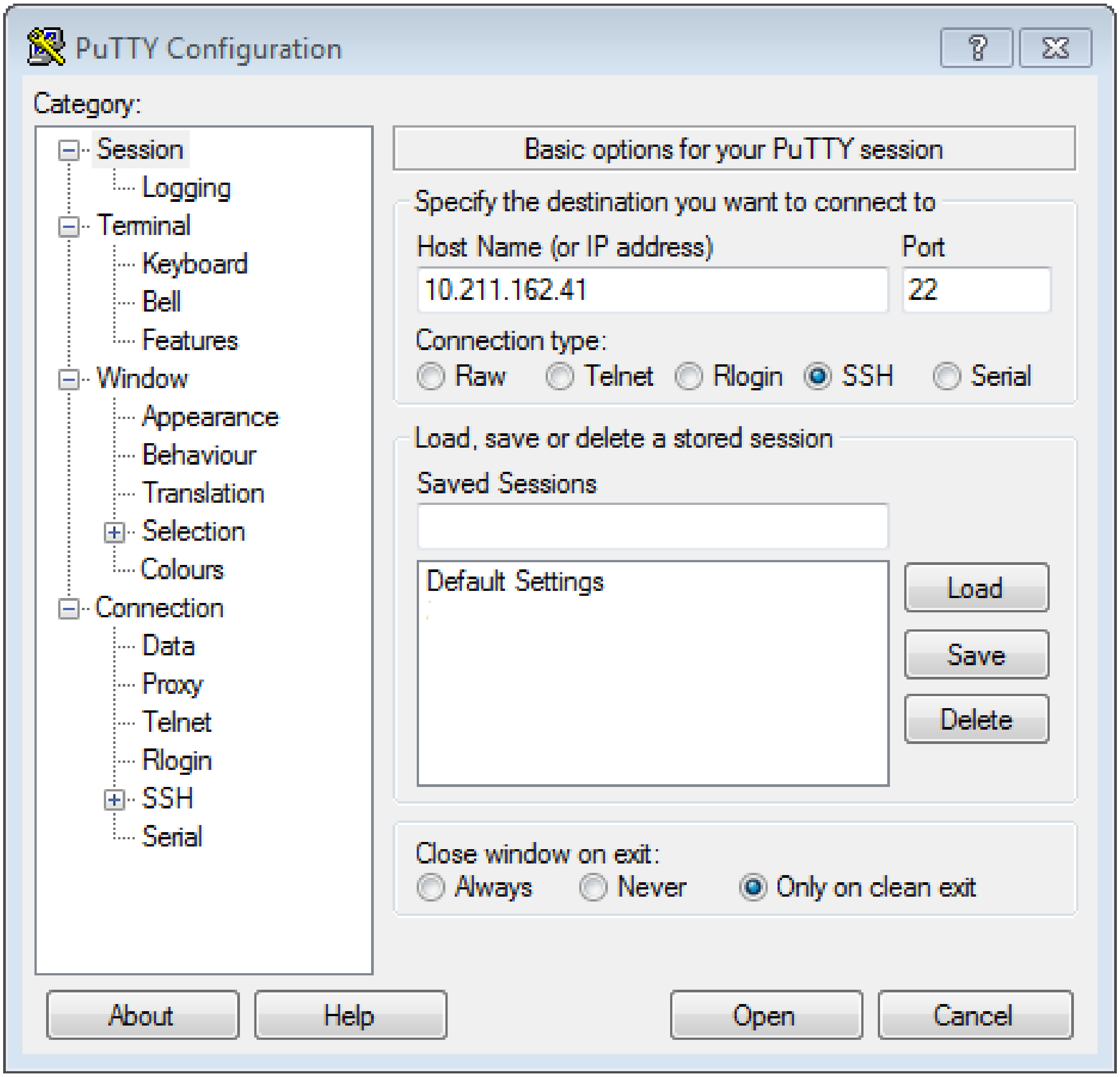
Creating TLS Certificate with SAN

This section describes how to create a TLS certificate with Subject Alternative Name (SAN). SAN extension of the certificate specifies additional host names so that more than one host can use the same copy of a single certificate. This is required because the traffic between FXS ports and the SBC uses the loopback 127.0.0.1 address.

Connecting CA to the MX-ONE Server

To connect Certificate Authority (CA) to the MX-ONE server:

1. Log into the SSH client, such as Putty.
2. Connect to the MX-ONE server using the administrator credentials:



MX-ONE Server - SSH

Verifying the CA File

Using the command line, verify that the certificate authority file is valid and contains the required Issuer:

```
openssl x509 -in /etc/opt/eri_sn/certs/root/CA.pem -text| grep Issuer
```

```
Issuer: CN=MXOneEnterpriseCA, C=SG, O=Root Certificate, OU=MX-ONE/emailAd-
dress=root@EXLIMIPV4V6.mxonebglman.com
```

Generating the Unit Certificate with SAN

For the TLS to be enabled on different interfaces you must generate a unit certificate with SAN. For example:

- Uplink: 10.211.162.127
- LAN1: 192.168.0.10 (default IP)
- Loopback: 127.0.0.1 (IP to connect FXS and PSTN ports to the internal SBC)

The certificate must be generated on the MX-ONE server using the following procedure:

1. Create a directory for the unit certificates.

```
mkdir -p /etc/opt/eri_sn/certs/units
cd /etc/opt/eri_sn/certs/units
```

2. Create a configuration file for the uplink (10.211.162.127.cnf) to provide SAN options. Replace the uplink IP (10.211.162.127) with the IP address of the EX and GX controller.

```
cat << EOF > 10.211.162.127.cnf
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
CN = 10.211.162.127

[v3_req]
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = 192.168.0.10
DNS.2 = 127.0.0.1
DNS.3 = 10.211.162.127
IP.1 = 192.168.0.10
IP.2 = 127.0.0.1
IP.3 = 10.211.162.127
EOF
```

3. Generate a Private Key for the EX and GX controller unit. The first command will generate a key with password, the second one will convert the key so it requires no password (required by the following steps):

```
openssl genrsa -aes256 -out 10.211.162.127.key.protected 2048
openssl rsa -in 10.211.162.127.key.protected -out 10.211.162.127.key
```

4. Generate a CSR for the Unit.

```
openssl req -new -key 10.211.162.127.key -out 10.211.162.127.csr -sha256
-config 10.211.162.127.cnf
```

5. Verify the CSR:

```
openssl req -text -noout -verify -in 10.211.162.127.csr
```

6. Sign the CSR and generate a new certificate:

```
openssl x509 -req -sha256 -days 3652 -in 10.211.162.127.csr -CA
../root/CA.pem -CAkey ../root/private_key.pem -CAserial ../root/CA.srl
-CAcreateserial -out 10.211.162.127.crt -extfile 10.211.162.127.cnf
-extensions v3_req
```

7. Verify the uplink certificate (10.211.162.127.crt):

```
openssl x509 -in 10.211.162.127.crt -text
```

8. Create the uplink .pem file.

```
cat 10.211.162.127.crt 10.211.162.127.key > 10.211.162.127.pem
```

9. Generate a Private Key for the EX and GX controller unit. The first command will generate a key with password, the second one will convert the key so it requires no password (required by the following steps):

```
openssl genrsa -aes256 -out 10.211.162.127.key.protected 2048
openssl rsa -in 10.211.162.127.key.protected -out 10.211.162.127.key
```

10. Generate a CSR for the Unit.

```
openssl req -new -key 10.211.162.127.key -out 10.211.162.127.csr -sha256
-config 10.211.162.127.cnf
```

11. Verify the CSR:

```
openssl req -text -noout -verify -in 10.211.162.127.csr
```

12. Sign the CSR and generate a new certificate:

```
openssl x509 -req -sha256 -days 3652 -in 10.211.162.127.csr -CA
../root/CA.pem -CAkey ../root/private_key.pem -CAserial ../root/CA.srl
-CAcreateserial -out 10.211.162.127.crt -extfile 10.211.162.127.cnf
-extensions v3_req
```

13. Verify the uplink certificate (10.211.162.127.crt):

```
openssl x509 -in 10.211.162.127.crt -text
```

14. Create the uplink .pem file.

```
cat 10.211.162.127.crt 10.211.162.127.key > 10.211.162.127.pem
```

Copying the Files on PC

Using a file transfer software, copy the following files from the MX-ONE to your PC:

- Unit Certificate: /etc/opt/eri_sn/certs/units/10.211.162.127.pem
- Root Certificate: /etc/opt/eri_sn/certs/root/CA.pem

Configuring the EX/GX for TLS

The procedures described in this section shows how to configure TLS in an EX/GX controller to establish a secure connection with MX-ONE system.

Login to the EX/GX Controller

Open a Web browser, log in to the EX/GX controller by using the default IP address or the previously configured uplink IP address. You can either log in as a public user (with no password) or an administrator using default credentials.

Installing Unit Certificates

1. In the EX/GX controller user interface, navigate to **Management > Certificates**.

System | Network | SIP Proxy | SBC | ISDN | POTS | SIP | Media | Telephony | Call Router | Management

Configuration Scripts | Backup / Restore | Firmware | Certificates | Virtuo | SNMP | CWMP | Access Control | File

• **Certificates**

Certificate transfer through web browser is disabled because of unsecure HTTP access.

- Activate unsecure certificate transfer through web browser

2. Under Certificate Import Through Web browser.
   a. Choose **Host** and click **Choose**.
   b. Select the appropriate file (.pem file) on your PC and then click **Import**.

Certificate Import Through Web Browser		
Type	**Path**	
Host ▼	Choose File 10.211.162.127.pem	Import

3. Under Certificate Import Through Web browser.
   a. Choose **Other** and click **Choose**.
   b. Select the appropriate file (.pem file) on your PC and then click **Import**.

Certificate Import Through Web Browser		
Type	**Path**	
Other ▼	Choose File CAmx.pem	Import

4. Verify that the certificates have been installed:

Some changes require to restart a service to apply new configuration.
Please click this link to access the services table or just restart required services

• **Certificates**

Host Certificates

File Name	Issued To	Issued By	Valid From	Valid To	Usage
10.211.162.127.pem	10.211.162.127	MXOneEnterpriseCA	2019-08-09 14:40:22	2029-08-08 14:40:22	TlsClient, TlsServer

Other Certificates

File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA
CAmx.pem	MXOneEnterpriseCA	MXOneEnterpriseCA	2019-08-07 14:58:23	2020-08-06 14:58:23		Yes
Cert_MxDefault001.der	Media5 Corporation - Mediatrix Primary CA	Media5 Corporation - Mediatrix Primary CA	2015-03-06 15:06:40	2065-03-06 15:06:40	TlsClient, TlsServer	Yes

Host Certificate Associations

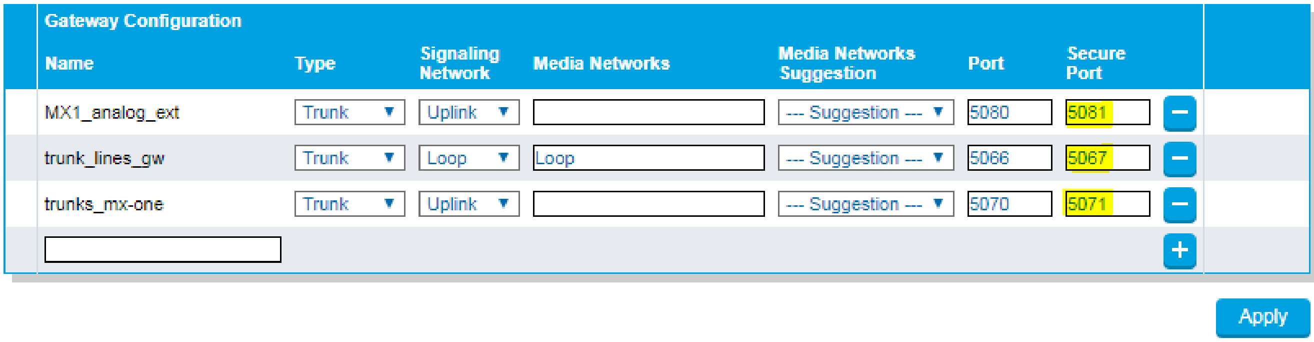
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert	Nlm	SBC	CWMP
10.211.162.127.pem	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

5. Restart required services and log in to the EX/GX controller user interface again.

Configuring the Secure SIP ports

By default, the EX/GX controllers only listen to the non-secure SIP ports.

1. Navigate to **SIP > Gateways** in the EX/GX controller interface.



2. For each SIP Gateway, add a secure port (Port +1).
3. Click **Apply** and restart the services.

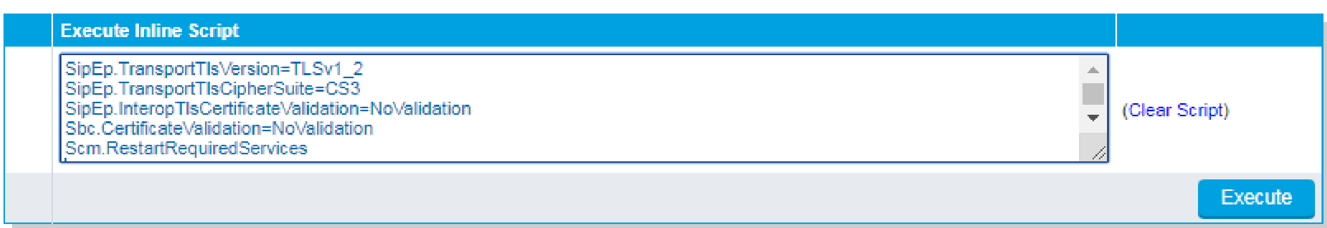
Setting the TLS version, Cipher Suite, and Certificate Validation Level

For SIP gateways on the EX/GX to communicate with the SBC service, configure the TLS version to 1.2 and the Cipher Suite to CS3.

NOTE: It is recommended to disable the certificate validation until the setup is complete.

1. Navigate to **Management > Configuration Scripts** and click Execute.
2. Select **Activate unsecure script transfers and execution through web browser**.
3. In Execute inline script, copy and paste the following:

```
SipEp.TransportTlsVersion=TLSv1_2
SipEp.TransportTlsCipherSuite=CS3
SipEp.InteropTlsCertificateValidation=NoValidation
Sbc.CertificateValidation=NoValidation
Scm.RestartRequiredServices
```



4. Click **Execute**. It takes approximately 30 seconds for the services to restart.

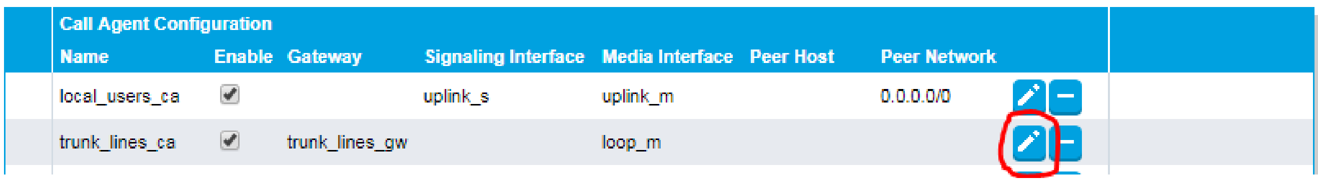
Enabling TLS on the SBC Service

To enable TLS on SBC:

1. Navigate to **SBC > Configuration**.

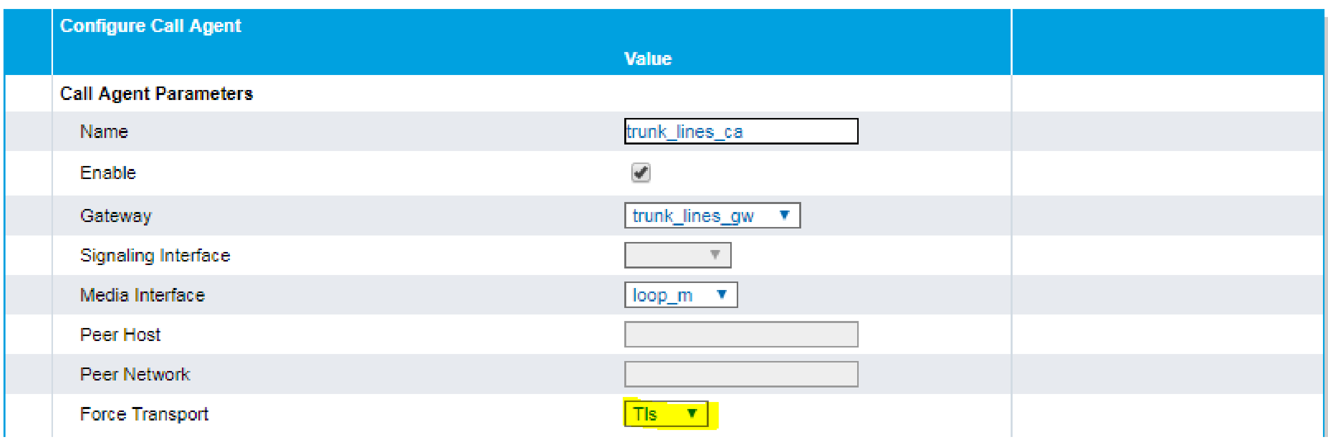
• **Configuration**

2. In Call Agent Configuration, edit trunk_lines_ca by clicking on the Edit icon next to it.

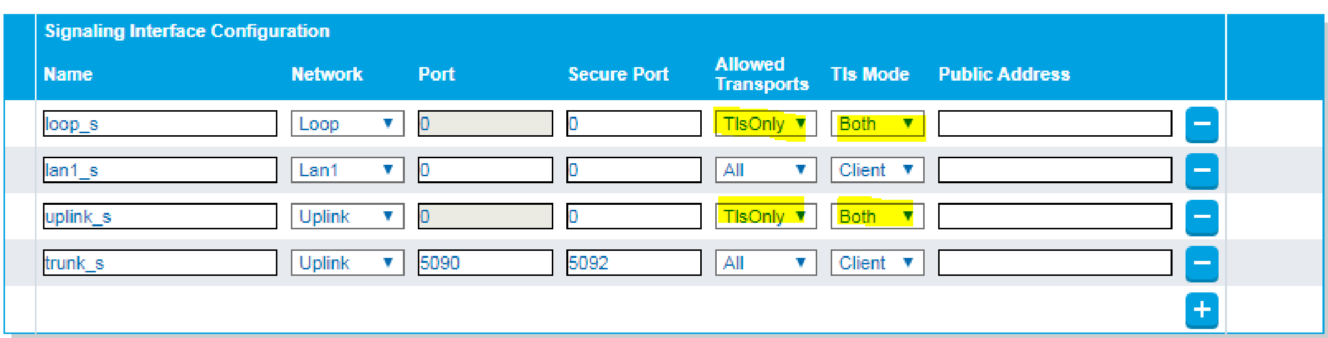


3. Set Force Transport as **Tls** and click **Save**.

• **Configure Call Agent**



4. Repeat the above steps for `local_users_ca` and `MX-ONE_LIM1` call agents.
5. In Signaling Interface Configuration, `edit loop_s`and `uplink_s`and set Allowed Transports to **TlsOnly** and **Tls Mode** to **Both** and click **Apply**.

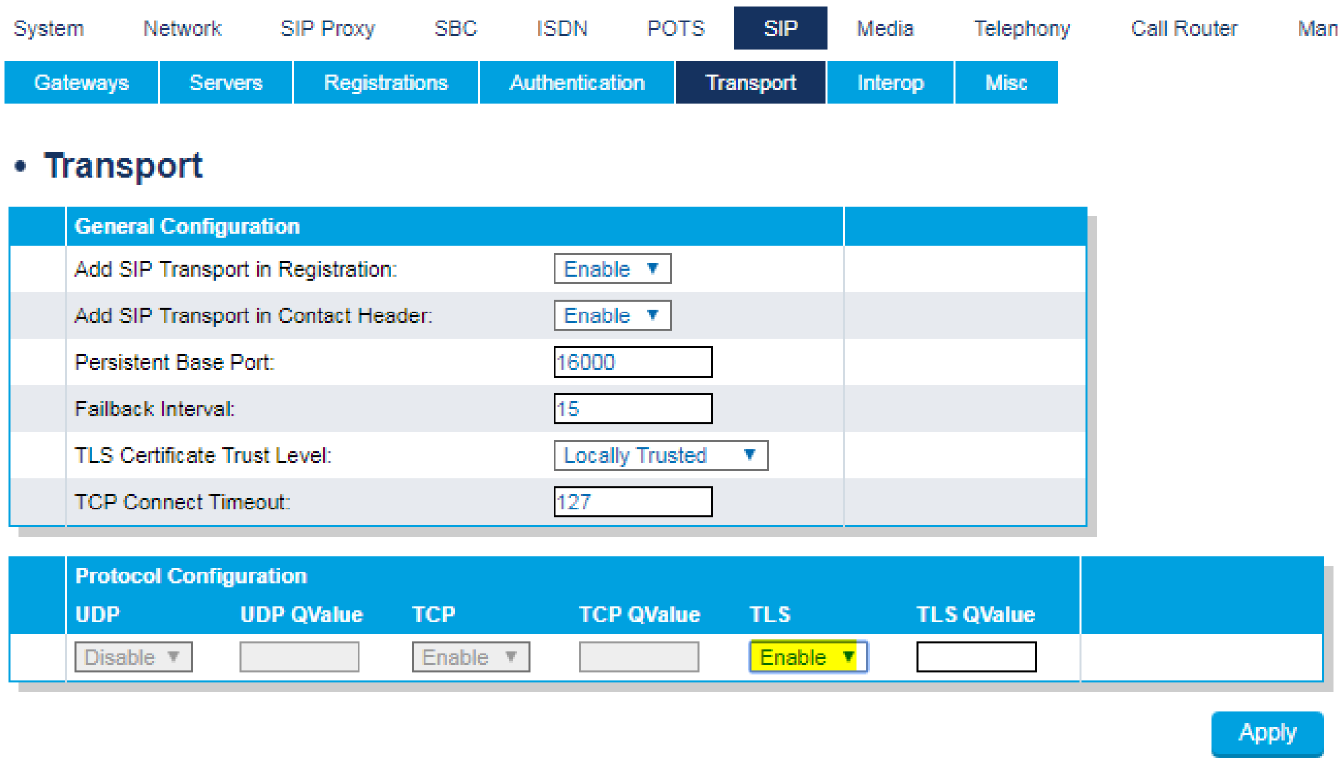


6. Restart the required services. It takes about 30 seconds for the SBC service to restart.
7. Clear cache registration by navigating to **SBC > Registration**.

Enabling TLS between SIP Gateways and SBC

To enable TLS between SIP Gateways and SBC:

1. Navigate to **SIP > Transport.**



2. Configure the general configuration details as shown in the above figure and click **Apply.**
3. Restart the required services. It takes about 30 seconds for the service to restart.
4. Navigate to **SIP > Registrations**.
5. Validate if endpoints are registered the agent MX1_analog_ext.
6. Navigate to **SBC > Registration**, validate all endpoints are registered using TLS.

AoR	Contact-URI
sip:32100@10.211.162.41	sip:32100@10.211.162.127:16000;transport=tls
sip:32101@10.211.162.41	sip:32101@10.211.162.127:16000;transport=tls
sip:32102@10.211.162.41	sip:32102@10.211.162.127:16000;transport=tls
sip:32103@10.211.162.41	sip:32103@10.211.162.127:16000;transport=tls

7. Test a call between endpoints. For example 32100 to 32101.

Enabling SRTP on EX/GX Controller

To enable SRTP on the EX/GX controller:

1. Navigate to **Media > Security**.
2. Under Select Endpoint, choose **Secure**.
3. Select Mode as, **Secure**.
4. Select Key Management Protocol as, **SDES**.
5. Select Encryption as, **AES_CM_128**.
6. Select **Yes** for the T.38 setting.

Enabling Certificate Validation

After the EX/GX controller with TLS setup is complete, you can enable certificate validation:

1. Navigate to **Management > Configuration Scripts > Execute** and select Activate unsecure script transfers and execution through web browser.
2. In Execute Inline Script, copy and paste the following:

```
SipEp.InteropTlsCertificateValidation=HostName
bc.CertificateValidation=HostName
Sbc.ResetRegistrationCache
Scm.RestartRequiredServices
```

3. Click **Execute**.
4. Navigate **SIP > Registrations**.
5. Validate that the endpoints are registered to call agent `MX1_analog_ext`.

Known Limitations

Below are some known limitations when using the EX-Controller or GX-Gateway:

- When MX-ONE is installed as a virtual machine in the EX-Controller, Provisioning Manger is not allowed to be installed.
- When EX-Controller is used in a multi-server configuration the EX-controller can never be the master server.
- Maximum 5 servers can exist in a multi-server configuration, where at least one of the servers is an EX-controller.
- When deploying a MX-ONE as a virtual machine the maximum amount of RAM is 7168 Mbytes.